



15. 2. 227





MÉMOIRES

DE MATHÉMATIQUE ET DE PHYSIQUE,

PAR GUILLAUME LIBRI.

TOME PREMIER.



FLORENCE,
CHEZ LÉONARD CIARDETTI.
1829.

GUILLAUME LIBRI

OFFRE CET OUVRAGE

A Sa Mère

ROSE LIBRI.

PRÉFACE.

L'essai que je publie maintenant, contient une partie des recherches que je fais depuis dix ans sur les diverses branches de l'analyse. Dès mes premiers pas dans l'étude des mathématiques, m'étant spécialement occupé de la théorie des nombres (*), je pensai que les obstacles que l'on rencontrait en traitant les problèmes numériques venaient, pour la plupart, du manque de méthode, et de l'état d'isolement dans lequel se trouvait cette branche de l'algèbre; je dirigeai par conséquent mes efforts vers l'unique but de découvrir un principe général qui renfermât toute la théorie des nombres, et qui permît de mettre en équation tous les problèmes numériques sans négliger aucune des conditions nécessaires, de manière qu'ils ne dûssent présenter d'autres difficultés que celles qui dérivent de l'état actuel de l'analyse; difficultés qui, sous des formes différentes, se reproduisent dans tous les problèmes de mathématique transcendante. Mais à mesure que je tâchais d'avancer dans mon entreprise, je voyais les obstacles se multiplier autour de moi; car il me fallait attaquer la question principale, et créer en même tems des ressources analytiques pour effectuer les opérations que le nouveau point de vue, sous lequel j'envisageais le

(*) Voyez *Memoria di Guglielmo Libri sopra la teoria dei numeri. Firenze* 1820.

problème, me rendait nécessaires. C'est ainsi que j'ai dû traiter les questions en apparence les plus disparates, mais qui en effet concourent toutes au même but. D'un autre côté je voyais aussi le sujet s'agrandir sans cesse entre mes mains, et je trouvais des relations qui jusque là avaient été inobservées. En réunissant peu à peu tous ces matériaux, je m'aperçus que l'analyse indéterminée n'était qu'une branche de la théorie générale des fonctions entières ; théorie qui est du plus haut intérêt dans les mathématiques. En effet, elle renferme l'analyse indéterminée, le développement des fonctions, l'intégration des équations aux différences (et par conséquent l'intégration des équations différentielles), la résolution des équations numériques, la théorie des fonctions discontinues, le calcul des probabilités, et enfin une théorie nouvelle et fort délicate sur la comparaison des différens ordres d'irrationalité; théorie qui sert à résoudre un grand nombre de questions importantes.

Arrivé à ce point j'aurais voulu réunir mes recherches dans un seul ouvrage, et traiter complètement toutes les questions que présente la théorie des fonctions entières. Mais ce n'était pas tout d'avoir trouvé le principe général; il fallait après cela attaquer les difficultés analytiques, parfois insurmontables, qu'offre chaque problème en particulier. D'ailleurs le mauvais état de ma santé m'ayant forcé d'interrompre souvent ce travail, et me laissant peu d'espoir de l'achever, du moins pour le moment, j'ai dû abandonner l'idée de former un traité complet des fonctions entières, et je me suis décidé à publier séparément quelques-uns des mémoires que j'ai écrits à différentes époques, sur les diverses questions que je voulais résoudre. Plusieurs de ces mémoires ont été présentés à l'Institut de France, et doivent paraître dans le recueil des Savans Etrangers; les journaux en ont rendu compte dans le tems, et quelques géomètres en ont eu connaissance. Et comme l'impression de ce volume, à cause de différens obstacles,

traîne depuis deux ans, il se pourrait que d'autres analystes eussent fait paraître dans cet intervalle, des recherches analogues à celles que je publie ici; mais en confrontant les dates, il serait aisé de voir que je n'ai rien emprunté a personne.

Des six mémoires que je publie dans ce volume, cinq regardent la théorie des fonctions entières; un seul est relatif à la théorie de la chaleur, et je le donne seulement comme une ébauche d'un travail plus général que je prépare sur cette matière: d'ailleurs il fournit les premiers élemens d'un mémoire, que je fairai paraître dans la suite, sur l'application de la théorie des nombres aux problèmes de physique mathématique. Tant que l'analyse indéterminée a été séparée des autres branches des mathématiques, elle ne leur paraissait fournir aucun secours; mais en se liant à l'algèbre ordinaire, elle doit servir à son avancement. Déjà dans ce volume j'expose quelques-unes des relations qui existent, entre la théorie des nombres et celle des fonctions circulaires; et l'on verra dans la suite, comment ces rapports servent à trouver la valeur d'un grand nombre d'intégrales définies, valeur que l'on aurait calculée difficilement par d'autres moyens. Je montre aussi la manière d'appliquer le calcul d'approximation aux équations indéterminées, ce que l'on avait jusqu'à présent regardé comme impossible, quoique, au contraire, dans le seul cas de l'analyse indéterminée, les méthodes d'approximation donnent des solutions exactes.

Il me serait fort difficile de présenter ici l'analyse des matières que j'ai traitées dans les mémoires compris dans ce volume: car tout ce que je publie maintenant étant nouveau, ou par la méthode que j'ai suivie, ou par les résultats que j'ai obtenus, il me faudrait répéter à présent tout ce que je dis dans le cours du volume. D'ailleurs chaque mémoire est précédé d'une courte introduction qui suffit pour donner une idée des matières que j'y traite; ce qui vaut beaucoup

mieux qu'une introductiou générale, à cause du peu de lien apparent qui existe entre les divers sujets traités dans ces mémoires.

Ce volume ne renferme que des préliminaires, et je me suis attaché surtout à traiter les problèmes dont la résolution pourra m'être nécessaire dans la suite. J'ai négligé les détails, parceque je n'écrivais point un livre élémentaire, et j'ai tâché plutôt de faire saisir l'esprit de mes méthodes que d'en développer toutes les parties. On trouvera que quelquefois je suis parvenu à de nouveaux résultats, en modifiant une méthode connue pour l'appliquer à un problème nouveau; mais c'est ici le seul genre de plagiat que je me sois permis, et au lieu de m'en cacher je l'avoue le premier. Car je pense que les méthodes sont pour l'esprit ce que les instrumens sont pour les bras, et que dans toutes les sciences il faut se former une table des méthodes connues, pour les appliquer dans l'occasion à de nouveaux faits, de même que l'on applique en chymie les divers réagens connus à un corps inconnu, pour l'analyser et le réduire à ses élémens les plus simples. De cette manière on parvient aux formules générales, qui sont les machines de la pensée, et qui forment d'elles-mêmes le tissu, pourvu qu'on leur fournisse la matière. Lorsqu'après avoir essayé toutes les méthodes connues, on voit qu'elles ne suffisent pas pour résoudre la question proposée, il faut se créer de nouveaux instrumens et de nouvelles méthodes; et je me flatte que mon ouvrage n'en est pas entièrement dépourvu.

Si l'essai que je publie à présent est accueilli avec quelque indulgence par les géomètres, je ferai paraître d'autres volumes qui contiendront des recherches sur différentes branches d'analyse et de physique. A la fin de ce volume j'indique les titres des mémoires qui sont déjà presqu'en état d'être imprimés, et j'y ajoute, pour prendre date, sous la forme de problèmes, l'énoncé de quelques propositions nouvelles que j'ai démontrées.

Il me reste à parler d'une chose: mes compatriotes trouveront peut-être étrange que j'aie écrit cet essai en français. Personne n'aime sa patrie plus que moi; mais cet ouvrage, qui par sa nature ne doit avoir qu'un très-petit nombre de lecteurs, resterait absolument inconnu dans les pays où l'analyse mathématique est cultivée avec le plus de succès, s'il n'était écrit dans la langue qui est la plus généralement connue en Europe. Ainsi je ne dois que prier mes lecteurs de me pardonner les fautes qui, sans doute, me seront échappées en écrivant dans une langue étrangère.

Florence le 16 Janvier 1829.

TABLE DES MÉMOIRES.

Mémoire sur quelques formules générales d'analyse . . Page 1
Mémoire sur la théorie de la chaleur 15
Mémoire sur les fonctions discontinues 34
Mémoire sur la théorie des nombres 47
Mémoire sur la résolution de quelques équations indéterminées . . 141
Mémoire sur la résolution des équations indéterminées à l'aide des séries 169
Annonces de mémoires qui paraîtront dans la suite 201

MÉMOIRE

SUR QUELQUES FORMULES GÉNÉRALES D'ANALYSE.

INTRODUCTION.

L'algèbre présente un grand nombre de problèmes, tels que le développement du polynome, la recherche des fonctions symétriques des racines des équations algébriques, l'élimination, etc., dont la solution dépend dans chaque cas particulier des principes les plus élémentaires, mais qui offrent de grandes difficultés quand il s'agit de les résoudre en général. Cependant le défaut de formules se fait sentir chaque fois que la solution d'un problème exige, que l'on connaisse le résultat général des opérations qu'on sait effectuer seulement dans les cas particuliers; et comme cette circonstance se renouvelle souvent dans l'analyse, il en résulte une imperfection qui plane sur toute l'étendue de la science. Cette imperfection disparaîtrait si l'on savait, dans le développement d'un polynome quelconque, trouver le terme général sans qu'il fût besoin de connaître les termes précédens, comme cela parait nécessaire au premier abord; car cette question renferme toutes celles de la même espèce que nous avons énoncées ci-dessus. Les géomètres allemands, qui se sont beaucoup occupés de ces recherches, ont tâché de tirer le développement du polynome de l'analyse combinatoire, dont Leibnitz avait donné la première idée; mais leurs procédés qui reposent presqu'entièrement sur la partition des nombres, (opération qu'on ne sait pas effectuer en général) ne peuvent fournir que des règles didactiques, et point de formules générales. D'autres analystes ont ramené ce problème au calcul différentiel et aux intégrales définies: ces méthodes qui sont plus directes, exigent cependant que l'on connaisse les différentielles successives de certaines fonctions; et comme pour les obtenir il faut développer ces fonctions en séries, il est clair que le problème revient en dernière analyse à ce qu'il était d'abord, puisque il faut calculer les termes précédens pour avoir celui que l'on cherche. Ainsi jusqu'à présent, il n'y avait aucune formule générale, qui offrît sous une forme concise tous les termes dont le développement d'une fonction polynome se compose, sans qu'il fût nécessaire

de faire aucune opération préliminaire. Cependant il semble que dans l'état actuel de l'analyse il faut renoncer à tous les moyens pratiques, comme l'on a depuis long tems abandonné les constructions graphiques pour la solution des problèmes; et que l'on doit chercher des formules générales, qui aient pour caractère spécial de résoudre la question dans sa plus grande étendue, sans qu'il soit nécessaire, pour les appliquer aux cas particuliers, d'effectuer, d'autre opération que celle d'y substituer les quantités connues. Chaque fois qu'une formule ne remplit pas ces conditions, elle est incomplète; parceque la valeur d'une quantité qui en dépendrait, ne saurait être substituée dans une autre expression.

Pour résoudre les questions qui nous occupent, nous avons ramené d'abord le développement d'un polynome à une équation aux différences d'ordre indéfini, dont l'intégrale exprimée en série nous a donné le terme général du développement cherché: puis nous avons partagé cette série en autant d'autres séries partielles qu'il y a de facteurs dans les termes qui la composent; et nous avons pu de cette manière en obtenir la somme en termes finis. La formule que l'on trouve ainsi, est presqu'aussi simple que celle qui exprime l'intégrale de l'équation linéaire aux différences du premier ordre, et lui ressemble à quelques égards. On en déduit de suite une expression des nombres de Bernoulli, plus complète et moins difficile à calculer que toutes celles que l'on connaissait jusqu'à présent. Ceci nous conduit à exposer une formule assez simple, qui sert à développer par les puissances ascendantes de la variable, l'intégrale finie d'une fonction quelconque.

La méthode dont nous avons fait usage pour développer le polynome, sert encore à trouver la somme des puissances des racines d'une équation algébrique quelconque; on obtient dans ce cas deux développemens, qui en dernière analyse sont identiques, et on les somme de la même manière que la série que l'on avait obtenue pour le polynome. Nous déduisons des formules qui représentent ces développemens, une expression générale de la somme des diviseurs d'un nombre quelconque; somme que l'on n'avait jamais pu soumettre à aucune loi régulière: et nous montrerons dans la suite comment ces mêmes formules peuvent servir à trouver directement un nombre premier plus grand qu'une limite quelconque. Lorsqu'on connait la somme des puissances des racines d'une équation, toutes les autres fonctions symétriques des mêmes racines s'en déduisent: mais nous n'avons pas cru nécessaire de nous arrêter à exposer les formules qui les représentent. Cependant nous avons pensé qu'il ne serait pas tout à fait inutile de

donner la formule générale d'élimination, entre deux équations algébriques de degrés quelconques; et nous l'avons exposée en négligeant la démonstration qui est très-facile a retrouver.

Les formules que nous exposons dans ce mémoire, offrent l'avantage de pouvoir introduire dans le calcul, sous forme finie, le résultat d'opérations qui dépendent de développemens très-longs à effectuer. Nous avons cru nécessaire de les placer à la tête de ces recherches, à cause des applications fréquentes que nous en ferons dans la suite, à l'analyse numérique et à diverses questions de calcul intégral.

ANALYSE.

Etant proposé de développer suivant les puissances ascendantes de z, le polynome indéfini

$$\left(1+a_1 z+a_2 z^2 \ldots\ldots + a_x z^x + \text{etc.}\right)^m = 1 + y_1 z + y_2 z^2 \ldots\ldots + y_x z^x + \text{etc.},$$

si l'on prend la différentielle logarithmique de chacun des membres de cette équation, et que l'on égale les coefficiens des mêmes puissances de z, on aura la suite d'équations aux différences

$$y_1 = ma_1;$$
$$2y_2 = 2ma_2 + (m-1)a_1 y_1;$$
$$3y_3 = 3ma_3 + (2m-1)a_2 y_1 + (m-2)a_1 y_2;$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$(1)\ldots\ldots xy_x = xma_x + \left((x-1)m-1\right)a_{x-1}y_1 + \left((x-2)m-2\right)a_{x-2}y_2 + \text{etc.};$$

et en substituant dans la dernière, les valeurs de y_1, y_2, y_3, etc., déduites des équations précédentes, on aura l'intégrale de l'équation (1) exprimée en série de cette manière

$$(2)\ldots y_x = \frac{xma_x}{x} + \left((x-1)m-1\right)\frac{a_{x-1}}{x}(ma_1) + \left((x-2)m-2\right)\frac{a_{x-2}}{x}\left(\frac{2ma_2+(m-1)a_1(ma_1)}{2}\right)$$
$$\ldots\ldots\ldots\ldots\ldots + \left((x-t)m-t\right)\frac{a_{x-t}\,\beta_t}{x} + \text{etc.},$$

et il sera facile de saisir la loi des termes, puisque le coefficient β_t, est égal à la somme de tous les termes précédens dans lesquels on a changé x et t.

A l'aide des substitutions successives on peut toujours exprimer en série l'intégrale d'une équation aux différences; mais les formules que l'on obtient de cette manière manquent de symétrie, et ne peuvent pas aisément se représenter à l'esprit; pour les rendre utiles il faut les réduire à une forme finie, et c'est ce que nous allons faire maintenant.

Si dans l'équation (2) on réunit par groupes les termes composés de deux, de trois,.... de $u+1$ facteurs, (en ne considérant comme facteurs que les coefficiens indéterminés $a_1, a_2, a_3, \ldots a_x$, etc., du polynome) et si l'on désigne ces groupes par $A_2, A_3, \ldots A_{u+1}$, etc., on aura

$$y_x=\begin{cases} \dfrac{xma_x}{x} \\ +\Big((x-1)m-1\Big)\dfrac{a_{x-1}}{x}(ma_1)+\Big((x-2)m-2\Big)\dfrac{a_{x-2}}{x}(ma_2)+\Big((x-3)m-3\Big)\dfrac{a_{x-3}}{x}(ma_3)\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots+\Big((x-t)m-t\Big)\dfrac{a_{x-t}}{x}(ma_t)+\text{etc.} \\ +\Big((x-2)m-2\Big)\dfrac{a_{x-2}}{x}\left(\dfrac{(m-1)a_1(ma_1)}{2}\right)+\Big((x-3)m-3\Big)\dfrac{a_{x-3}}{x}\left(\dfrac{(2m-1)a_2(ma_1)+(m-2)a_1(ma_2)}{3}\right)+\text{etc.} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots+\text{etc.} \end{cases}$$

$$=\frac{xma_x}{x}+A_2+A_3\ldots\ldots\ldots\ldots+A_{u+1}+\text{etc.}$$

Maintenant le groupe A_2 a pour terme général l'expression $\frac{1}{x}ma_{x_1}\Big((x-x_1)m-x_1\Big)a_{x-x_1}$ dans laquelle x_1 reçoit successivement les valeurs $1, 2, 3, \ldots x-1$; l'on aura donc

$$A_2=\sum\frac{1}{x}ma_{x_1}\Big((x-x_1)m-x_1\Big)a_{x-x_1},$$

en intégrant entre les limites $x_1=1$, $x_1=x$. Le groupe A_3 a pour terme général

$$\frac{m}{x.x_1}a_{x_2}\Big((x-x_1)m-x_1\Big)a_{x-x_1}\Big((x_1-x_2)m-x_2\Big)a_{x_1-x_2},$$

où il faut donner à x_1 toutes les valeurs $2, 3, 4, \ldots\ldots x-1$; et faire successivement $x_2=1, 2, 3, \ldots\ldots x_1-1$; on trouvera par conséquent

$$A_3=\sum\sum\frac{m}{x.x_1}a_{x_2}\Big((x-x_1)m-x_1\Big)a_{x-x_1}\Big((x_1-x_2)m-x_2\Big)a_{x_1-x_2},$$

en intégrant entre les limites

$$x_1=2,\ x_1=x;\ x_2=1,\ x_2=x_1.$$

Et en général on aura l'équation

$$A_{u+1}=$$

$$\sum\sum\sum \cdots \frac{m}{x.x_1.x_2\ldots x_{u-1}}\, a_{x_u}\Big((x-x_1)m-x_1\Big)a_{x-x_1}\Big((x_1-x_2)m-x_2\Big)a_{x_1-x_2}\cdots\Big((x_{u-1}-x_u)m-x_u\Big)a_{x_{u-1}-x_u},$$

où il faut intégrer entre les limites

$$x_1=u,\ x_1=x;\ x_2=u-1,\ x_2=x_1;\ x_3=u-2,\ x_3=x_2;\ \ldots\ x_u=1,\ x_u=x_{u-1}.$$

En exprimant les intégrales définies aux différences par la notation de M.r Fourier, on aura

$$A_{u+1}=\sum_{x_1=u}^{x_1=x}\ \sum_{x_2=u-1}^{x_2=x_1}\cdots\sum_{x_u=1}^{x_u=x_{u-1}} \frac{m}{x.x_1.x_2\ldots x_{u-1}}\, a_{x_u}\left\{\begin{array}{l}\Big((x-x_1)m-x_1\Big)a_{x-x_1}\Big((x_1-x_2)m-x_2\Big)a_{x_1-x_2}\ldots\ldots \\ \ldots\ldots\ldots\ldots\Big((x_{u-1}-x_u)m-x_u\Big)a_{x_{u-1}-x_u}\end{array}\right\};$$

mais comme l'on a

$$\sum_{x_1=u}^{x_1=x}\ \sum_{x_2=u-1}^{x_2=x_1}\cdots\cdots\sum_{x_u=1}^{x_u=x_{u-1}} = e^{\sum_{s=1}^{s=u+1}\log\sum_{x_s=u-s+1}^{x_s=x_{s-1}}},$$

e étant la base des logarithmes hyperboliques, et que l'on a aussi par la notation de Vandermonde

$$\frac{1}{x.x_1\ldots x_{u-1}}\Big((x-x_1)m-x_1\Big)a_{x-x_1}\Big((x_1-x_2)m-x_2\Big)a_{x_1-x_2}\ldots\ldots\Big((x_{u-1}-x_u)m-x_u\Big)a_{x_{u-1}-x_u}$$

$$=\left[\frac{1}{x_{u-1}}\Big((x_{u-1}-x_u)m-x_u\Big)a_{x_{u-1}-x_u}\right]^u$$

(pourvu que l'on suppose $x_0=x$)

on trouvera

$$A_{u+1}=e^{\sum_{s=1}^{s=u+1}\log\sum_{x_s=u-s+1}^{x_s=x_{s-1}}}\ ma_{x_u}\left[\frac{1}{x_{u-1}}\Big((x_{u-1}-x_u)m-x_u\Big)a_{x_{u-1}-x_u}\right]^u$$

et puisque

$$y_x = ma_x + \sum_{u=1}^{u=x} A_{u+1} \quad ,$$

on obtiendra enfin

$$(3) \ldots\ldots y_x = ma_x + \sum_{u=1}^{u=x} e^{\sum_{s=1}^{s=u+1} \log \sum_{x_s=u-s+1}^{x_s=x_{s-1}}} ma_{x_0} \left[\frac{1}{x_{u-1}} \Big((x_{u-1} - x_u) m - x_u \Big) a_{x_{u-1} - x_u} \right]^u$$

en faisant $x_0 = x$. (*)

On peut encore réduire cette expression à la forme suivante

$$y_x = ma_x + m \sum_{u=1}^{u=x} e^{\sum_{s=1}^{s=u+1} \log \sum_{x_s=u-s+1}^{x_s=x_{s-1}}} a_{x_0} \, e^{\sum_{s=0}^{s=u} \log \frac{1}{x_s} \big((x_s - x_{s+1}) m - x_{s+1} \big) a_{x_s - x_{s+1}}}$$

en exprimant toujours par e la base des logarithmes hyperboliques, et faisant $x_0 = x$.

On sait qu'étant donnée la série

$$\frac{z}{e^z - 1} = \frac{1}{1 + \frac{z}{1.2} + \frac{z^2}{1.2.3} \ldots + \frac{z^x}{1.2.3 \ldots (x+1)} + \text{etc.}} = 1 + y_1 z + y_2 z^2 \ldots\ldots + y_x z^x + \text{etc.} ;$$

(*) Nous aurions pu nous épargner cette réduction, en écrivant x_0 au lieu de x dans tout ce qui précède; mais nous ne l'avons pas fait, à cause des difficultés typographiques, que nous aurions rencontrées dans l'impression des formules exposées dans ce mémoire ; difficultés que le manque des caractères nécessaires rend plus grandes en Toscane qu'ailleurs.

les nombres de Bernoulli seront exprimés par la relation

$$B_x = 1.2.3\ldots\ldots(x+1)y_{x+1}.$$

Si à présent on fait dans la formule (3)

$$a_{x_u} = \frac{1}{1.2.3\ldots(x_u+1)} = \frac{1}{\overset{x_u+1}{[x_u+1]}};$$

et $m = -1$; on aura

$$B_{x-1} = \overset{x}{[x]}y_x = -\overset{x}{[x]}\left\{\frac{1}{\overset{x+1}{[x+1]}} + \sum_{u=1}^{u=x} e^{\sum\limits_{s=1}^{s=u+1} \log \sum\limits_{x_s=u-s+1}^{x_s=x_{s-1}}} \frac{(-1)^u}{\overset{x_u+1}{[x_u+1]}}\left[\frac{1}{\overset{x_{u-1}-x_u+1}{[x_{u-1}-x_u+1]}}\right]^u\right\}$$

$$= 1.2.3\ldots x\left\{\begin{array}{l} -\dfrac{1}{1.2.3\ldots(x+1)} - \dfrac{1}{1.2.3\ldots\ldots x}\left(-\dfrac{1}{1.2}\right) - \dfrac{1}{1.2.3\ldots(x-1)}\left(-\dfrac{1}{1.2.3} - \dfrac{1}{1.2}\left(-\dfrac{1}{1.2}\right)\right)\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots - \dfrac{1}{1.2}\left(-\dfrac{1}{1.2.3\ldots x} - \dfrac{1}{1.2.3\ldots(x-1)}\left(-\dfrac{1}{1.2}\right) - \text{etc.}\right). \end{array}\right\}$$

En faisant dans cette expression successivement $x = 1, 2, 3$, etc., on obtiendra les valeurs déjà connues

$$B_0 = -\tfrac{1}{2};\ B_1 = 2\left(-\tfrac{1}{6} + \tfrac{1}{4}\right) = \tfrac{1}{6};$$
$$B_2 = 6\left(-\tfrac{1}{24} + \tfrac{1}{12} + \tfrac{1}{12} - \tfrac{1}{8}\right) = 0;\ \text{etc.}$$

Cette formule est assez simple, et le calcul numérique, pour chaque cas particulier, en est plus aisé que dans les expressions connues jusqu'à présent : d'ailleurs elle est générale, et fournit même la valeur de $B_0 = -\frac{1}{2}$, que d'autres formules (celle de La Place par exemple) ne donnent pas : nous l'avons rapportée comme une application très-simple du développement du polynome que nous venons de trouver.

Les nombres de Bernoulli ne sont au fond autre chose que les coefficiens des diverses puissances de la variable dans le développement de $\sum z^n$, multipliés

par des nombres connus: s'il s'agissait de développer la fonction indéterminée $\Sigma\,\varphi(z)$ par les puissances ascendantes de z, on aurait un résultat assez simple que nous allons faire connaître.

Etant donnée l'équation

$$\varphi(z) = e_0 + e_1 z + e_2 z^2 \ldots\ldots + e_x z^x + \text{etc.},$$

elle se réduit à

$$e^{uz} = 1 + uz + \frac{u^2 z^2}{1.2} \ldots\ldots + \frac{u^x z^x}{1.2.3\ldots\ldots x} + \text{etc.},$$

lorsque $\varphi(z) = e^{uz}$, et on aura dans ce cas

$$e_0 = 1;\ e_1 = u;\ e_2 = \frac{u^2}{1.2};\ldots\ldots e_x = \frac{u^x}{1.2.3\ldots.x};\ \text{etc.}.$$

Si l'on fait à présent

$$(4)\ldots\ldots \Sigma\,\varphi(z) = a_1 z + a_2 z^2 \ldots\ldots\ldots + a_x z^x + \text{etc.},$$

$$\Sigma\ e^{uz} = b_1 z + b_2 z^2 \ldots\ldots\ldots + b_x z^x + \text{etc.},$$

a_x sera une fonction linéaire des coefficiens e_{x-1}, e_x, e_{x+1}, etc., et b_x sera une fonction semblable des coefficiens

$$\frac{u^{x-1}}{1.2.3\ldots(x-1)},\ \frac{u^x}{1.2.3\ldots x},\ \frac{u^{x+1}}{1.2.3\ldots(x+1)},\ \text{etc.},$$

et les diverses puissances de u, u^2, u^3, etc, resteront indépendantes les unes des autres, de même que les coefficiens e_0, e_1, e_2, ... e_x; et il ne pourra pas y avoir de réduction, de telle manière que si l'on connait la valeur de b_x, on trouvera celle de a_x en substituant

$$1.2.3\ldots\ x\ e_x = \frac{d^x.\varphi(v)}{dv^x}$$

(où il faut faire $v=0$ après les différentiations) au lieu de u^x.

Maintenant l'on a $\Sigma\ e^{uz} = \dfrac{e^{uz}-1}{e^u-1}$, et comme nous avons trouvé précédemment le développement de

$$\frac{1}{e^u-1} = \frac{1}{u} + y_1 + y_2 u + y_3 u^2 + \text{etc.};$$

on aura

$$\Sigma\, e^{uz} = \left(\frac{1}{u} + y_1 + y_2 u + y_3 u^2 \ldots + y_x u^{x-1} + \text{etc.}\right)\left(uz + \frac{u^2 z^2}{1.2} + \frac{u^3 z^3}{1.2.3} \ldots + \frac{u^x z^x}{1.2.3\ldots x} + \text{etc.}\right)$$

$$= b_1\, z + b_2\, z^2 \ldots\ldots + b_x\, z^x + \text{etc.},$$

et par suite

$$b_x = \frac{u^{x-1}}{1.2.3\ldots x} + \frac{y_1\, u^x}{1.2.3\ldots x} + \frac{y_2\, u^{x+1}}{1.2.3\ldots x} + \text{etc.}$$

Si l'on substitue dans cette équation $\frac{d^x . \varphi(v)}{dv^x}$ au lieu de u^x, on aura en général

$$a_x = \frac{1}{1.2.3\ldots x}\left(\frac{d^{x-1} . \varphi(v)}{dv^{x-1}} + y_1 \frac{d^x . \varphi(v)}{dv^x} + y_2 \frac{d^{x+1} . \varphi(v)}{dv^{x+1}} + \text{etc.}\right).$$

Ce coefficient peut aussi s'exprimer en termes finis de cette manière

$$a_x = \frac{1}{1.2.3\ldots\ldots x}\left(\frac{d . \varphi(v)}{dv}\right)^x \left(e^{\frac{d.\varphi(v)}{dv}} - 1\right)^{-1};$$

pourvu qu'en développant on change $\left(\frac{d . \varphi(v)}{dv}\right)^p$ en $\frac{d^p . \varphi(v)}{dv^p}$, comme on le fait pour d'autres formules de la même espèce. Alors en substituant dans l'équation (4) les valeurs de a_1, a_2, a_3, etc., exprimées de cette manière, on aura la formule

$$\Sigma\, \varphi(z) = \left(z \frac{d . \varphi(v)}{dv} + \frac{z^2}{1.2}\left(\frac{d . \varphi(v)}{dv}\right)^2 \ldots + \frac{z^x}{1.2.3\ldots x}\left(\frac{d . \varphi(v)}{dv}\right)^x + \text{etc.}\right)\left(e^{\frac{d.\varphi(v)}{dv}} - 1\right)^{-1}$$

$$= \left(e^{z\frac{d.\varphi(v)}{dv}} - 1\right)\left(e^{\frac{d.\varphi(v)}{dv}} - 1\right)^{-1},$$

dans laquelle il faut changer $\left(\frac{d . \varphi(v)}{dv}\right)^p$ en $\frac{d^p . \varphi(v)}{dv^p}$, après avoir développé, et

faire $v=0$, après les différentiations. On pourra développer de la même manière $\sum^2\varphi(z)$; et en général $\sum^n\varphi(z)$, $\Delta^n\varphi(z)$, etc.

Etant donnée l'équation

$$x^n - a_1\, x^{n-1} - a_2\, x^{n-2} \,\ldots\ldots - a_n = 0\,,$$

si l'on exprime par P_m la somme des puissances m.^{mes} de ses racines, on a toujours

$$(5)\ldots\ldots P_m = a_1\, P_{m-1} + a_2\, P_{m-2}\,\ldots\ldots\ldots\ldots + m\,a_m\,,$$

et par suite

$$P_{m-1} = a_1\, P_{m-2} + a_2\, P_{m-3}\,\ldots\ldots\ldots\ldots + (m-1)\,a_{m-1}\,,$$
$$P_{m-2} = a_1\, P_{m-3} + a_2\, P_{m-4}\,\ldots\ldots\ldots\ldots + (m-2)\,a_{m-2}\,,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{etc.}\,,$$

et si l'on substitue ces dernières valeurs dans l'équation (5) il en résultera la formule

$$P_m = ma_m + (m-1)\,a_{m-1}\,(a_1) + (m-2)\,a_{m-2}\big(a_2 + a_1\,(a_1)\big)\ldots\ldots\ldots + (m-t)\,a_{m-t}\,\beta_t + \text{etc.}\,,$$

dans laquelle le coefficient β_t se forme en changeant m en t dans tous les termes précédens, et négligeant tous les coefficiens numériques externes. Si l'on avait commencé par substituer les valeurs de P_1, P_2, P_3, etc., dans l'équation (5), on aurait obtenu l'expression

$$P_m = ma_m + a_{m-1}\,(a_1) + a_{m-2}\big(2a_2 + a_1\,(a_1)\big) + a_{m-3}\Big(3a_3 + a_2(a_1) + a_1\,\big(a_2 + a_1\,(a_1)\big)\Big) + \text{etc.}\,,$$

qui ne diffère de la précédente, que par la disposition des termes dont elle se compose.

On doit observer que ces formules sont exactes seulement pour des valeurs de m entières, positives, et plus grandes que zéro; et qu'il faut s'arrêter lorsqu'on trouve des coefficiens à indices plus petits que l'unité. Lorsque $m=0$, on a $P_0=n$, et si m a une valeur négative, on divisera l'équation proposée par $a_n\, x^n$, et en faisant $\frac{1}{x}=y$, on cherchera la somme des puissances $-m$.^{mes} des racines de la nouvelle équation en y qui en résultera.

Si l'on décompose la série qui exprime la valeur de P_m, en autant de séries partielles qu'il peut y avoir de facteurs algébriques, on aura

$$P_m = \left\{ \begin{array}{l} \quad ma_m \\ +(m-1)\,a_{m-1}\,(a_1)+(m-2)\,a_{m-2}\,(a_2)+(m-3)\,a_{m-3}\,(a_3) \;+\text{ etc.} \\ +(m-2)\,a_{m-2}\,(a_1)\;(a_1)+(m-3)\,a_{m-3}\;(a_2\;a_1+a_1\;a_2) \;+\text{ etc.} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \;+\text{ etc.} \end{array} \right\},$$

et on trouvera aisément, comme on l'a fait pour le polynome,

$$P_m = m\,a_m + \sum_{x=1}^{x=m} e^{\sum\limits_{s=1}^{s=x+1} \log \sum\limits_{m_s=x-s+1}^{m_s=m_{s-1}}} (m-m_1)\,a_{m_0}\left[a_{m_{s-1}-m_s}\right]^{\bar{x}},$$

en faisant toujours $m_0 = m$.

Il est clair que l'on pourra écrire aussi

$$P_m = ma_m + \sum_{x=1}^{x=m} e^{\sum\limits_{s=1}^{s=x+1} \log \sum\limits_{m_s=x-s+1}^{m_s=m_{s-1}}} (m-m_1)\,a_{m_0}\; e^{\sum\limits_{s=0}^{s=x} \log a_{m_s-m_{s+1}}},$$

et ces deux expressions seront équivalentes. En appliquant cette formule à l'équation

$$(x-1)^{-n}\,(x^n-1)(x^{n-1}-1)(x^{n-2}-1)\ldots\ldots(x^2-1)(x-1)=0,$$

et en indiquant par $\int(n)$ la somme des diviseurs de n, on aura par la notation

de Vandermonde l'expression

$$\int(n)-n=$$

$$\left\{\begin{array}{l}
n\left\{-\left([n+n-1]^{n}[0]^{-n}-[n+n-2]^{n-1}[0]^{1-n}-[n+n-3]^{n-2}[0]^{2-n}\ldots\pm\left[n+n-\tfrac{1}{2}(3z^2\pm z)-1\right]^{n-\frac{1}{2}(3z^2\pm z)}\left[\;0\;\right]^{\frac{1}{2}(3z^2\pm z)-n}\ldots\text{etc.}\right)\right\}\\
+(n-1)\left\{-\left([n+n-2]^{n-1}[0]^{1-n}-[n+n-3]^{n-2}[0]^{2-n}-[n+n-4]^{n-3}[0]^{3-n}\ldots\pm\left[n+n-\tfrac{1}{2}(3z^2\pm z)-2\right]^{n-1-\frac{1}{2}(3z^2\pm z)}\left[\;0\;\right]^{\frac{1}{2}(3z^2\pm z)+1-n}\ldots\text{etc.}\right)\right\}\left(-\left([n]^{1}[0]^{-1}-[n-1]^{0}[0]^{-0}\right.\right.\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
+(n-u)\left\{-\left([n+n-u-1]^{n-u}[0]^{u-n}-[n+n-u-2]^{n-u-1}[0]^{u-n+1}\ldots\ldots\pm\left[n+n-u-\tfrac{1}{2}(3z^2\pm z)-1\right]^{n-u-\frac{1}{2}(3z^2\pm z)}\left[\;0\;\right]^{\frac{1}{2}(3z^2\pm z)+u-n}\ldots\ldots\text{etc.}\right)\right\}A_u\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\text{etc.}
\end{array}\right.$$

dans laquelle la loi des termes est manifeste, puisque le coefficient A_u se forme en changeant en u la seconde n comprise entre les crochets des factorielles, dans tous les termes qui le précèdent, et en faisant $n=u$ dans tous les exposans de ces mêmes factorielles: pourvu que l'on égale à l'unité tous les coefficiens numériques externes (tels que n, $n-1$, $n-2$, etc.,) des termes précédens. Ainsi par exemple un terme de la forme $\pm(n-s)\,[n+n-s-1]^{n-s}[0]^{s-n}$, se changera en celui-ci $\pm[n+u-s-1]^{u-s}[0]^{s-u}$. Il est clair que toutes ces séries s'arrêteront lorsque dans un terme quelconque de la forme $[n+A-1]^{A}[0]^{-A}$, A sera un nombre entier négatif.

Ainsi par exemple en faisant dans cette formule successivement $n=1$, $n=2$, $n=3$, etc., on aura

$$\int(1) = 1 - \left({[1]}^{1}{[0]}^{-1} - {[0]}^{0}{[0]}^{-0}\right) = 1 - 1 + 1 = 1\,,$$

$$\int(2) = 2 - 2\left({[3]}^{2}{[0]}^{-2} - {[2]}^{1}{[0]}^{-1} - {[1]}^{0}{[0]}^{-0}\right) + \left({[2]}^{1}{[0]}^{-1} - {[1]}^{0}{[0]}^{-0}\right)\left({[2]}^{1}{[0]}^{-1} - {[1]}^{0}{[0]}^{-0}\right)$$

$$= 2 - 2\left(\frac{3.2}{1.2} - 2 - 1\right) + (2-1)(2-1) = 2 - 0 + 1 = 3\,.$$

$$\int(3) = 3 - 3\left({[5]}^{3}{[0]}^{-3} - {[4]}^{2}{[0]}^{-2} - {[3]}^{1}{[0]}^{-1}\right) + 2\left({[4]}^{2}{[0]}^{-2} - {[3]}^{1}{[0]}^{-1} - {[2]}^{0}{[0]}^{-0}\right)\left({[3]}^{1}{[0]}^{-1} - {[2]}^{0}{[0]}^{-0}\right)$$

$$+ \left({[3]}^{1}{[0]}^{-1} - {[2]}^{0}{[0]}^{-0}\right)\left({[4]}^{2}{[0]}^{-2} - {[3]}^{1}{[0]}^{-1} - {[2]}^{0}{[0]}^{-0} - \left({[3]}^{1}{[0]}^{-1} - {[2]}^{0}{[0]}^{-0}\right)^{2}\right)$$

$$= 3 - 3\left(\frac{5.4.3}{1.2.3} - \frac{4.3}{1.2} - 3\right) + 2\left(\frac{4.3}{1.2} - 3 - 1\right)(3-1) + (3-1)\left(\frac{4.3}{1.2} - 3 - 1 - (3-1)^{2}\right)$$

$$= 3 - 3(10 - 6 - 3) + 2(6-4)2 + 2(6-4-4) = 3 - 3 + 8 - 4 = 4\,.$$

. . . . etc.

S'il s'agissait de déterminer les coefficiens de l'équation

$$x^{n} + A_{1}\,x^{n-1} + A_{2}\,x^{n-2} \ldots\ldots\ldots + A_{n} = 0\,,$$

dont les racines sont connues, en indiquant par P_{z_0} la somme des puissances z_0.^{mes} de ses racines, on aurait

$$A_{z_0} = -\frac{1}{z_0}\,P_{z_0} - \frac{1}{z_0}\sum_{x=1}^{x=z_0} e^{\sum\limits_{s=1}^{s=x+1}\log\sum\limits_{z_s=x-s+1}^{z_s=z_{s-1}}} P_{z_0}\left[\frac{1}{z_s}P_{z_{s-1}-z_s}\right]^{x}(-1)^{x}\,.$$

Etant proposé d'éliminer y entre les deux équations

$$y^{m} + e_{1}\,y^{m-1} + e_{2}\,y^{m-2} \ldots\ldots\ldots\ldots + e_{m} = 0\,;$$
$$y^{n} + b_{1}\,y^{n-1} + b_{2}\,y^{n-2} \ldots\ldots\ldots\ldots + b_{n} = 0\,;$$

l'équation résultante après l'élimination sera celle-ci

$$(6)\ldots\ldots 1+\sum_{t_0=1}^{t_0=mn+1}\left\{\begin{array}{l}\dfrac{1}{t_0}P_{t_0}A_{t_0-1}\\[2em] +\displaystyle\sum_{x=1}^{x=t_0} e^{\sum\limits_{s=1}^{s=x+1}\log\sum\limits_{t_s=x-s+1}^{t_s=t_{s-1}}\frac{1}{t_x}P_{t_x}A_{t_x-1}\,e^{\sum\limits_{z=0}^{z=x}\log\left(\frac{1}{t_z}P_{t_z-t_{z+1}}A_{t_z-t_{z+1}-1}\right)}}\end{array}\right\}.$$

Dans cette formule A_ν représente le coefficient de z_ν dans le développement de la fraction

$$\frac{b_1+2\,b_2\,z+3b_3\,z^2\,\ldots\ldots\ldots+nb_n\,\,z^{n-1}}{1+\,b_1\,z+\,b_2\,z^2\,\ldots\ldots\ldots+\,b_n\,\,z^n}\,,$$

et P_q exprime la somme des puissances $-q$.[mes] des racines de l'équation

$$y^m+e_1\,y^{m-1}+e_2\,y^{m-2}\,\ldots\ldots\ldots+e_m=0\,;$$

et comme les valeurs de A_ν et de P_q peuvent se déduire des formules que nous avons trouvées précédemment, on substituera ces valeurs dans l'équation (6) et le problème sera résolu complètement.

Nous avons trouvé depuis long-temps les formules démontrées dans ce mémoire: elles ont été exposées dans deux mémoires que nous avons présentés en 1823, et en 1825, à l'Académie Royale des Sciences de Paris.

MÉMOIRE

SUR LA THÉORIE DE LA CHALEUR.

INTRODUCTION.

Lorsque l'illustre géomètre, qui le premier a découvert les lois de la propagation de la chaleur, s'occupa de cette théorie, les physiciens admettaient presque géuéralment, que le refroidissement des corps s'opère d'après la différence qui passe entre leur température, et celle du milieu environnant. Depuis cette époque MM. Dulong et Petit sout parvenus, par des expériences délicates et variées, à découvrir la véritable loi d'après laquelle la chaleur se propage à la surface des corps. Cette loi remarquable, et entièrement différente de celle que Newton avait énoucée, paraissait devoir exciter l'attentiou des analystes, et les engager à connaître les modifications qu'elle introduirait dans les résultats du calcul: mais on a dû remarquer, que dans les recherches plus récentes qui out été publiées sur la théorie de la chaleur, on partait toujours de la loi de Newton.

Losqu'il s'agit de températures peu élevées, on peut supposer sans erreur sensible, que le refroidissement s'opère d'après la différeuce des températures; mais il n'en est pas de même dans le problème général, et quoiqu'on ait cru que l'erreur ne devenait apréciable qu'à des températures très-élevées, déjà à la chaleur de l'eau bouillante, on commet une erreur de presque deux degrés du thermomètre centesimal, dans l'équation différentielle qui exprime le mouvement de la chaleur; et cette erreur qui affecte à la fois la valeur de l'inconnue, et la forme sous laquelle elle se trouve dans l'équation différentielle, doit devenir bien plus sensible dans l'intégrale. Il est vrai qu'en partant de la loi découverte par M. Dulong, les équations que l'on obtient ne peuveut plus être intégrées en termes finis avec les méthodes connues; mais il ne parait pas toujours permis dans les problèmes physiques de s'écarter de la nature, pour simplifier l'analyse qui sert à les résoudre: et d'ailleurs si une première approximation est suffisante pour les inventeurs d'une théorie, il faut que des recherches ultérieures rapprochent d'avantage le calcul de l'expérience. C'est ainsi que Newton ayant découvert

le système du monde, il a fallu un siècle de recherches pour construire l'édifice dont il avait posé les fondemens.

Dans le mémoire que nous publions à présent, nous nous sommes proposés de déterminer le mouvement linéaire de la chaleur, en partant de la loi du refroidissement découverte par M.r Dulong. On sait que cette loi se compose de deux parties, dont l'une exprime la perte de la chaleur éprouvée par l'effet du rayonnement, et l'autre représente l'action du milieu. Or cette seconde partie est sujette à des variations qu'il est très-difficile de soumettre au calcul: pour y parvenir il faudrait connaître la théorie des mouvemens des fluides élastiques; mais ce problème considéré dans sa généralité surpasse les forces actuelles de l'analyse. On a supposé, pour surmonter cette difficulté, que les corps dont on voulait connaître les changemens de température, étaient soumis à l'action d'un courant d'air de densité et de température constantes, qui frappait tous les points de leur surface avec une vitesse uniforme; mais il est aisé de voir l'impossibilité de vérifier en nature cette hypothèse, de manière qu'on ne peut tirer de là aucun résultat comparable à l'expérience. Pour rapprocher autant qu'il est possible la théorie de l'observation, nous avons dû considérer le mouvement linéaire de la chaleur, dans une armille de petite épaisseur renfermée dans un espace vide, dont l'enceinte est maintenue à une température constante. Ce problème conduit à une équation aux différentielles partielles qui n'est plus linéaire, et qui contient la variable principale sous la forme d'exponentielle. Il n'est plus possible dans ce cas d'intégrer directement l'équation trouvée, et il faut recourir aux méthodes d'approximation. On ne connait pas de métode pour intégrer par approximation les équations aux différentielles partielles: on peut à la verité exprimer leur intégrale en séries, et l'on parvient, à l'aide du théorème de M.r Fourier, à sommer ces séries lorsqu'elles dérivent d'équations linéaires à coefficiens constans; mais lorsque la série est trop compliquée pour pouvoir en obtenir le terme général, il est impossible de juger de sa convergence, et le problème reste sans solution. Nous avons tâché d'appliquer aux équations aux différentielles partielles, la métode d'approximation dont on se sert pour les équations différentielles ordinaires. On sait que pour intégrer les équations differentielles qui expriment les mouvemens des corps célestes, on fait usage de la méthode d'approximation successive, à l'aide de laquelle on les réduit à un nombre indéfini d'équations linéaires; mais il arrive que chaque intégration introduit des arcs de cercle qui détruisent l'effet de l'approximation. Les plus grands géomètres ont

tâché da vaincre cette difficulté, mais les méthodes qu'ils ont inventées, quoique très-ingénieuses, deviennent souvent impraticables à cause de la longueur excessive des calculs qu'elles demandent. Et d'ailleurs il est très-difficile de s'assurer, que parmi les termes qu'on néglige il n'en existe aucun qui devienne sensible au bout d'un tems très-long: de telle manière que ces méthodes exigent presqu'autant de sagacité pour les appliquer, qu'il fallait de génie pour les découvrir. Toutes ces difficultés paraissent devoir se retrouver dans les équations aux différentielles partielles; cependant si au lieu d'intégrer complètement la première des équations linéaires que nous avons obtenues, pour prendre des intégrales particulières des autres, comme on le fait pour les équations différentielles ordinaires, on commence par prendre des intégrales particulières, des premières équations que l'on veut considérer, et que l'on n'intègre complètement que celle à laquelle on veut arrêter l'approximation, on obtiendra le nombre de fonctions arbitraires qui est nécessaire pour satisfaire à toutes les conditions du problème, et on sera assuré, comme on le démontre directement, de pouvoir éviter toujours les arcs de cercle. Nous avons effectué le calcul que nous venons d'indiquer, sur les deux premières équations linéaires que fournit le problème, et nous avons trouvé une formule qui se compose de celle que M. Fourier avait déjà donnée, et d'un terme de correction multiplié par une petite quantité. En embrassant un plus grand nombre d'équations, on trouverait la même expression, plus des termes multipliés par les puissances ascendantes de la petite quantité par rapport à laquelle on a développé. La méthode que nous venons d'exposer, peut s'appliquer à l'intégration par approximation d'une classe assez étendue d'équations aux différentielles partielles; mais ces recherches ne sauraient trouver place ici, et elles formeront le sujet d'un mémoire particulier.

Parmi les nombreux corollaires que M. Fourier a déduits de son analyse, il en est un fort remarquable qui prouve, qu'après un tems considérable la demi-somme des températures de deux points diamétralement opposés dans l'armille, forme toujours une quantité constante, et égale à la température moyenne. Ce résultat a été confirmé avec assez de précision par l'expérience, et il était intéressant de voir comment on tirerait la même conséquence de la loi découverte par M. Dulong. En partant de la température donnée par notre formule nous obtenons le même théorème, et nous démontrons qu'il dérive également de l'hypothèse de Newton, et de la loi observée.

En supposant le refroidissement proportionnel à la différence des températures,

on trouve qu'en plongeant l'extrémité d'une barre de petite épaisseur dans une source constante de chaleur, lorsque l'équilibre des températures se sera établi, la distribution de la chaleur dans la barre pourra être exprimée par une courbe logarithmique. Si l'on part de la loi observée, on obtient une équation différentielle qui n'est plus linéaire, mais qui peut cependant s'intégrer, et dont l'intégrale fait voir que ce n'est que pour des températures très-peu élevées, que l'état permanent de la barre peut se représenter par une courbe logarithmique : lorsque la chaleur augmente, cet état dépendra d'une transcendante elliptique, et en général il sera donné par une transcendante d'un ordre d'autant plus élevé, que la température sera plus grande.

L'intégrale de l'équation différentielle, qui exprime l'état permanent des températures dans une barre très-mince, n'est propre qu'à donner les températures d'une partie de la barre comprise entre deux foyers successifs : cela est évident dans le cas du mouvement linéaire, et tient à ce que l'équation différentielle que l'on a trouvée, ne se vérifie pas aux points qui servent de foyers. Mais lorsqu'il s'agit d'un corps d'une figure quelconque, qui a été échauffé primitivement par plusieurs foyers situés à sa surface ou dans son intérieur, il devient difficile de séparer les diverses parties du corps, pour chacune desquelles l'intégrale que la théorie fournit doit se vérifier, et de déterminer les limites au delà desquelles elle donnerait une valeur fautive. Le corps se subdivise alors, par rapport à son état calorifique, en d'autres corps dont les surfaces de contact jouissent de la propriété du maximum, ou du minimum de température. La détermination de ces surfaces-limites conduit à trouver un gran nombre de propriétés importantes dans la théorie de la chaleur, comme nous le montrerons dans une autre occasion.

Lorsqu'on cherche à connaître le mouvement de la chaleur dans un corps, on exprime la température d'un point donné en fonction de ses coordonnées, et du tems écoulé ; mais pendant que le corps s'échauffe ou se refroidit, toutes ses molécules se déplacent à cause du changement de volume produit par les variations de la température. On a négligé jusqu'à présent, dans la théorie mathématique de la chaleur, l'altération du volume des corps ; mais ce phénomène, le plus remarquable et le plus constant de tous ceux qui dépendent de la chaleur, ne nous paraît pas de nature à être négligé. En considérant les dilatations linéaires, nous donnons la formule de correction, qui doit servir à déterminer les coordonnées du point dont on connaît la température.

Nous n'avons traité, dans ce mémoire, que les cas les plus simples de la théorie de la chaleur; mais nous nous proposons de reprendre ce travail dans la suite, et d'appliquer notre analyse à des questions plus compliquées.

ANALYSE.

Si l'on renferme une armille circulaire homogène de petite épaisseur, dans une sphère creuse, qui ne contienne ni air ni aucune autre espèce de gaz, de manière que le centre de l'armille coïncide avec le centre de la sphère, et si le rayon de celle-ci est beaucoup plus grand que le rayon de l'armille, les parois de la sphère étant d'ailleurs entretenues à une température constante quelconque, il résulte du principe de la communication de la chaleur, et de la loi du refroidissement découverte par M. Dulong, que le mouvement de la chaleur dans l'armille sera exprimé, à très-peu près, par l'équation

$$\frac{dv}{dt} - \frac{ad^2v}{dx^2} + c(p^v - 1) = 0,$$

dans laquelle v exprime l'excès de la température du point que l'on considère, sur la température de l'enceinte; x représente la distance, comptée sur l'armille même, de ce point à l'origine des coordonnées; t est le tems écoulé depuis que l'armille a abandonné l'état initial des températures; et p, a et c, sont des constantes dont la première a pour valeur $\sqrt[20]{1,165}$, et les deux autres se déterminent par l'expérience dans chaque cas particulier.

En effet, l'équation que M. Fourier a trouvée, en supposant que le refroidissement s'opère d'après la différence des températures, est de la forme

$$(7) \ldots\ldots\ldots\ldots \frac{dv}{dt} - \frac{ad^2v}{dx^2} + Cv = 0,$$

et en y substituant au lieu de Cv, le terme $c(p^v - 1)$ qui exprime la loi du refroidissement dans le vide, d'après les expériences de MM. Dulong et Petit, on aura l'équation

$$(8) \ldots\ldots\ldots\ldots \frac{dv}{dt} - \frac{ad^2v}{dx^2} + c(p^v - 1) = 0,$$

que nous avions déjà indiquée.

Avant d'aller plus loin, il convient d'examiner un résultat que l'on a obtenu en faisant $v=e^{-ct}u$ dans l'équation (7); car par cette substitution elle se transforme dans la suivante

$$\frac{du}{dt} - \frac{ad^2u}{dx^2} = 0,$$

qui est la même équation (7) dans laquelle on a supposé qu'il n'y avait aucune déperdition de chaleur à la surface; d'où il résulte que dans l'hypothèse de Newton, le refroidissement qui s'opère à la surface ne change pas la loi de la distribution de la chaleur. Mais comme il n'est pas possible d'effectuer une réduction semblable sur l'équation (8), qui dérive de la loi observée, il faudra admettre qu'en nature, même dans le mouvement linéaire, la distribution de la chaleur est troublée par l'effet de la déperdition qui a lieu à la surface.

Maintenant si l'on fait log $p=\delta$, l'équation (8) prendra la forme

$$\frac{dv}{dt} - \frac{ad^2v}{dx^2} + c(e^{\delta v}-1) = 0,$$

l'exposant $\delta=\frac{1}{30}\log\left(\frac{1165}{1000}\right)$ étant une très-petite quantité; et si l'on développe en série l'exponentielle dans cette équation, on aura

$$\frac{dv}{dt} - \frac{ad^2v}{dx^2} + c\delta v + \frac{c\delta^2v^2}{1.2} + \frac{c\delta^3v^3}{1.2.3} + \text{etc.} = 0,$$

et par suite, en faisant $c\delta=b$, on obtiendra

$$\frac{dv}{dt} - \frac{ad^2v}{dx^2} + bv + \frac{b\delta v^2}{1.2} + \frac{b\delta^2v^3}{1.2.3} + \text{etc.} = 0.$$

Si l'on fait à présent

$$v = V + \delta V_1 + \delta^2 V_2 + \delta^3 V_3 + \text{etc.},$$

et que l'on substitue cette valeur dans l'équation précédente, en ordonnant le résultat par les puissances ascendantes de δ, on trouvera

$$(9)\ldots 0=\frac{dV}{dt}-\frac{ad^2V}{dx^2}+bV+\delta\left(\frac{dV_1}{dt}-\frac{ad^2V_1}{dx^2}+bV_1+\frac{bV^2}{1.2}\right)+\delta^2\left(\frac{dV_2}{dt}-\frac{ad^2V_2}{dx^2}+bV_2+bVV_1+\frac{bV^3}{1.2.3}\right)+\text{etc.},$$

et en égalant à zéro séparément les coefficiens de chaque puissance de δ, on aura les équations

$$\frac{dV}{dt} - \frac{ad^2V}{dx^2} + bV = 0,$$

$$\frac{dV_1}{dt} - \frac{ad^2V_1}{dx^2} + bV_1 + \frac{bV^2}{1.2} = 0,$$

$$\frac{dV_2}{dt} - \frac{ad^2V_2}{dx^2} + bV_2 + bVV_1 + \frac{bV^3}{1.2.3} = 0,$$

. . . . etc.,

dont le nombre sera déterminé par l'exposant de la plus grande puissance de δ, que l'on veut considérer.

En intégrant la première de ces équations, on obtiendra la valeur de V qui étant substituée dans la seconde équation, servira à déterminer V_1 et ainsi de suite, en introduisant dans la dernière équation les valeurs des inconnues déduites des équations précédentes, on déterminera une nouvelle inconnue. Mais il faut observer, qu'au lieu de prendre l'intégrale complète de la première équation, pour la substituer dans la seconde, et puis intégrer complètement celle-ci, pour substituer encore la valeur de l'inconnue dans la suivante, et ainsi de suite, on pourra exprimer

$$V, V_1, V_2, V_3, \ldots\ldots V_{n-1},$$

par des intégrales particulières, et δ^n étant la dernière puissance de δ que l'on veut considérer, il suffira d'intégrer complètement l'équation multipliée par δ^n, qui comprendra les différentielles de V_n et les quantités connues V, V_1, V_2, ... V_{n-1}; car l'intégrale complète de cette équation, contiendra toutes les fonctions arbitraires, qui sont nécessaires à la résolution générale du problème.

Supposons par exemple que dans l'équation (9) on veuille avoir égard à la première puissance de δ seulement, et négliger toutes les autres; on aura les

deux équations

$$\frac{dV}{dt} - \frac{ad^2V}{dx^2} + bV = 0,$$

$$\frac{dV_1}{dt} - \frac{ad^2V_1}{dx^2} + bV_1 + \frac{bV^2}{1.2} = 0,$$

dans la première desquelles on prendra une valeur particulière de V, pour la substituer dans la seconde équation, que l'on devra intégrer complètement.

Maintenant, on sait que l'on satisfait à l'équation

$$\frac{dV}{dt} - \frac{ad^2V}{dx^2} + bV = 0,$$

en faisant $V = (\sin nx + \cos nx)e^{-(b+an^2)t}$; n étant une constante indéterminée. Si l'on substitue cette valeur de V dans l'équation

$$\frac{dV_1}{dt} - \frac{ad^2V_1}{dx^2} + bV_1 + \frac{bV^2}{1.2} = 0,$$

on aura

$$\frac{dV_1}{dt} - \frac{ad^2V_1}{dx^2} + bV_1 + \frac{b}{1.2}(\sin nx + \cos nx)^2 e^{-2(b+an^2)t}$$

$$= \frac{dV_1}{dt} - \frac{ad^2V}{dx^2} + bV_1 + \frac{b}{1.2}(1 + \sin 2nx)e^{-2(b+an^2)t} = 0,$$

et en faisant $V_1 = y\,e^{-2(b+an^2)t} + Z$, ($y$ étant fonction de x seulement, et Z fonction de x et de t) on obtiendra, après avoir divisé par $e^{-2(b+an^2)t}$,

$$2(b+an^2)y + \frac{ad^2y}{dx^2} - by - \frac{b}{1.2}(1+\sin 2nx) - \frac{dZ}{dt} + \frac{ad^2Z}{dx^2} - bZ = 0,$$

et si l'on égale à zéro séparement les termes qui contiennent Z, on aura après les réductions, les deux équations

$$\frac{d^2y}{dx^2} + \left(\frac{b}{a} + 2n^2\right)y = \frac{b}{2a}(1 + \sin 2nx),$$

$$(10) \ldots\ldots\ldots\ldots\ldots \frac{dZ}{dt} - \frac{ad^2Z}{dx^2} + bZ = 0,$$

dont la première a pour intégrale

$$y = \left\{ \begin{array}{l} \left(E_1 + \dfrac{b}{2a\sqrt{\dfrac{b}{a}+2n^2}} \displaystyle\int dx(1+\sin 2nx)\sin x\sqrt{\frac{b}{a}+2n^2}\right)\cos x\sqrt{\frac{b}{a}+2n^2} \\ + \left(E_2 - \dfrac{b}{2a\sqrt{\dfrac{b}{a}+2n^2}} \displaystyle\int dx(1+\sin 2nx)\cos x\sqrt{\frac{b}{a}+2n^2}\right)\sin x\sqrt{\frac{b}{a}+2n^2} \end{array} \right\};$$

et par suite on obtiendra

$$y = E_1 \cos y\sqrt{\frac{b}{a}+2n^2} + E_2 \sin x\sqrt{\frac{b}{a}+2n^2} - \frac{b}{2}\left(\frac{1}{b+2an^2} + \frac{\sin 2nx}{b-2an^2}\right).$$

Si l'on intègre à présent l'équation en Z, on aura

$$Z = \left(a_p \sin px + b_p \cos px\right) e^{-(b+ap^2)t},$$

a_p, b_p et p, étant des quantités quelconques; et comme l'équation (10) est linéaire et ne contient pas de terme indépendant de Z, il s'ensuit qu'elle sera satisfaite par une somme de termes semblables à la valeur de Z que nous avons déja trouvée, pourvu que les constantes a_p, b_p, p, soient différentes. Et par conséquent l'intégrale complète de l'équation (10) sera composée d'une suite infinie de valeurs semblables à celle que nous avons déja obtenue, pourvu que l'on change convenablement les constantes arbitraires.

Maintenant, puisque Z contient une infinité de constantes arbitraires, on pourra dans la valeur de y supprimer les deux constantes E_1, E_2, qui ne rendraient pas plus générale la valeur de V_1; alors en faisant $E_1 = E_2 = 0$, on aura une valeur de y qui ne contiendra plus les fonctions

$$\cos x\sqrt{\frac{b}{a}+2n^2}\quad;\quad \sin x\sqrt{\frac{b}{a}+2n^2}\quad;$$

Soit r le rayon de l'armille dans laquelle on suppose que la chaleur se propage; sa circonférence sera égale à $2r\pi$, et il est clair qu'en exprimant par v la température d'un point dont la distance à l'origine est x, la valeur de v ne devra pas changer lorsque dans la formule qui exprime v on mettra $x+2r\pi$, à la place de x : par conséquent il faudra, dans les valeurs de V, et de V_1, faire $n=\frac{m}{r}$, et $p=\frac{s}{r}$; m et s étant deux nombres entiers positifs quelconques: on aura donc, en négligeant les puissances supérieures de δ,

$$v=V+\delta V_1=V+\delta\left(y\, e^{-2(b+an^2)t}+Z\right)$$

$$=\left\{\begin{array}{l}\left(\sin\frac{mx}{r}+\cos\frac{mx}{r}\right)e^{-\left(b+\frac{am^2}{r^2}\right)t} \quad + \sum\limits_{s=0}^{s=\infty}\left(a_s\sin\frac{sx}{r}+b_s\cos\frac{sx}{r}\right)\delta\, e^{-\left(b+\frac{as^2}{r^2}\right)t} \\ \quad -\frac{br^2}{2}\left(\frac{1}{br^2+2am^2}+\frac{\sin\frac{2mx}{r}}{br^2-2am^2}\right)\delta\, e^{-2\left(b+\frac{am^2}{r^2}\right)t}\end{array}\right.$$

mais le premier terme $\left(\sin\frac{mx}{r}+\cos\frac{mx}{r}\right)e^{-\left(b+\frac{am^2}{r^2}\right)t}$ de cette formule pourra être compris sous le signe Σ, puisque la valeur de m devra se trouver parmi les valeurs de s; et en faisant $\delta a_s=A_s$, et $\delta b_s=B_s$, on aura

$$(11)\ldots\ldots V=\left\{\begin{array}{l}\sum\limits_{s=0}^{s=\infty}\left(A_s\sin\frac{sx}{r}+B_s\cos\frac{sx}{r}\right)e^{-\left(b+\frac{as^2}{r^2}\right)t} \\ -\frac{br^2}{2}\delta\left(\frac{1}{br^2+2am^2}+\frac{\sin\frac{2mx}{r}}{br^2-2am^2}\right)e^{-2\left(b+\frac{am^2}{r^2}\right)t}\end{array}\right\}$$

et cette formule exprimera le mouvement de la chaleur dans l'armille. Pour déterminer la fonction arbitraire ou, ce qui revient au même, la série des termes

$$A_1\ ,\ A_2\ ,\ A_3\ ,\ \ldots\ldots\ A_s\ ,\ \text{etc.}\ ,$$
$$B_1\ ,\ B_2\ ,\ B_3\ ,\ \ldots\ldots\ B_s\ ,\ \text{etc.}\ ,$$

on devra faire $t=0$, et on aura v égal à la température initiale, que nous exprimerons par la fonction $f(x)$, et qui étant développée en série suivant les sinus et cosinus des multiples de l'arc $\frac{x}{r}$ servira pour déterminer les coefficiens.

Si dans la formule (11) on fait $\delta=0$, on obtiendra l'expression que M. Fourier a trouvée le premier en partant de l'hypothèse de Newton. Pour déterminer m, on devra prendre le nombre entier le plus petit qui ne satisfait pas à l'équation

$$br^2 \pm 2\,am^2 = 0\,,$$

puisqu'on aura de cette manière la valeur la plus approchée, et on sera assuré de ne pas rencontrer des arcs de cercle qui détruiraient l'effet de l'approximation. Lorsque les conditions du problème permettront de faire $m=0$, le terme de correction, pour la première approximation, se réduira à $-\frac{\delta}{2}e^{-2bt}$; et on trouvera que ce terme est indépendant des coordonnées, et qu'il ne dépend que du tems.

On a vu qu'en faisant $E_1=E_2=0$, on obtenait

$$y=\frac{b}{2a\sqrt{\frac{b}{a}+2n^2}}\left\{\begin{array}{l}\cos x\sqrt{2n^2+\frac{b}{a}}\int dx\,(1+\sin 2nx)\sin x\sqrt{2n^2+\frac{b}{a}}\\[2ex] -\sin x\sqrt{2n^2+\frac{b}{a}}\int dx\,(1+\sin 2nx)\cos x\sqrt{2n^2+\frac{b}{a}}\end{array}\right\}$$

$$=-\frac{b}{2}\left(\frac{1}{b+2an^2}+\frac{\sin 2nx}{b-2an^2}\right)$$

de manière que les fonctions $\cos x\sqrt{\frac{b}{a}+2n^2}$, $\sin x\sqrt{\frac{b}{a}+2n^2}$,

s'évanouissaient d'elles-mêmes dans le calcul: il était nécessaire que cette réduction pût s'effectuer, autrement la température v ne serait pas restée la même en changeant x en $x+2r\pi$, dans la formule qui la représente. Cependant cette réduction, qui a paru un résultat de calcul, aura toujours lieu quel que soit le nombre des puissances de δ que l'on considère; en effet on a toujours l'équation

$$\cos ax\int dx\,\varphi(x)\sin ax-\sin ax\int dx\,\varphi(x)\cos ax$$

$$=-\frac{\varphi(x)}{a}-\frac{1}{a^2}\left(\cos ax\int dx\,\frac{d^2.\varphi(x)}{dx^2}\sin ax-\sin ax\int dx\,\frac{d^2.\varphi(x)}{dx^2}\cos ax\right)$$

$$=\frac{(-1)^p}{a^{2p}}\left(\cos ax\int dx\,\frac{d^{2p}.\varphi(x)}{dx^{2p}}\sin ax-\sin ax\int dx\,\frac{d^{2p}.\varphi(x)}{dx^{2p}}\cos ax\right)$$

$$-\frac{\varphi(x)}{a}+\frac{d^2.\varphi(x)}{a^3dx^2}-\frac{d^4.\varphi(x)}{a^5dx^4}\ldots\ldots+\frac{(-1)^p}{a^{2p-1}}\;\frac{d^{2p-2}.\varphi(x)}{dx^{2p-2}}\,;$$

qui montre, que si entre $\varphi(x)$, et $\frac{d^{2p}.\varphi(x)}{dx^{2p}}$ on peut avoir une équation de la forme $M\varphi(x)=\frac{d^{2p}.\varphi(x)}{dx^{2p}}$, M étant une quantité constante, on pourra toujours avoir

$$(12)\;\ldots\ldots\ldots\;\cos ax\int dx\,\varphi(x)\sin ax-\sin ax\int dx\,\varphi(x)\cos ax$$

$$=\left(\frac{a^{2p}}{a^{2p}-(-1)^pM}\right)\left(-\frac{\varphi(x)}{a}+\frac{d^2.\varphi(x)}{a^3dx^2}\ldots\ldots+\frac{(-1)^p}{a^{2p-1}}\;\frac{d^{2p-2}.\varphi(x)}{dx^{2p-2}}\right)$$

et l'on voit que le second membre ne contiendra ni $\cos ax$, ni $\sin ax$. Il est clair que si $\varphi(x)=A\sin mx+B\cos mx$, on pourra établir l'équation

$\frac{d^2.\varphi(x)}{dx^2} = -m^2\varphi(x)$, et par conséquent l'on obtiendra la valeur de l'intégrale (12) délivrée de sin ax, et de cos ax ; la même chose arrivera en général lorsque $\varphi(x)$ sera de la forme

$$A_1 \sin m_1 x + A_2 \sin m_2 x \ldots\ldots + A_t \sin m_t x + \text{etc.},$$
$$+ B_1 \cos m_1 x + B_2 \cos m_2 x \ldots\ldots + B_t \cos m_t x + \text{etc.},$$

et lorsqu'on aura

$$\varphi(x) = a + bx + cx^2 + dx^3 \ldots\ldots + ex^n ;$$

et dans d'autres cas.

Maintenant puisque les valeurs particulières de V, V_1, V_2, etc., peuvent toujours s'exprimer par des fonctions de la forme

$$e^{-lt}\left\{\begin{array}{l} P_1 \sin n_1 x + P_2 \sin n_2 x \ldots\ldots + P_q \sin n_q x \\ + Q_1 \cos n_1 x + Q_2 \cos n_2 x \ldots\ldots + Q_q \sin n_q x \end{array}\right\},$$

on sera toujours assuré que les sinus et cosinus des arcs irrationnels ne se trouveront pas dans l'intégrale complète, quel que soit le nombre des puissances de δ que l'on voudra considérer.

Il faut observer que si l'on avait $(-1)^p M - a^{2p} = 0$, le second membre de l'équation (12) aurait une valeur infinie : on rencontrerait cette circostance si l'un des nombres n_1, n_2, n_3, ... n_q, etc., compris dans les valeurs de V, V_1, V_2, etc., était égal à a ; alors en reprenant le calcul on trouverait, après les réductions, un terme de la forme $Nx \sin n_q x$, qui contiendrait l'arc de cercle x, et qui rendrait nul, dans le cas que nous considérons, l'effet de l'approximation : mais il est clair que le nombre m de la formule (11) pourra toujours être déterminé de manière que cela n'arrive pas, et il suffira à cet effet que le dénominateur ne soit pas zéro, comme nous l'avons déjà indiqué.

La formule (12) exige, pour être appliquée facilement, que la fonction $\varphi(x)$ puisse se réduire à une suite finie de monomes composés d'un seul facteur : cependant en poussant fort loin l'approximation, et en calculant un grand

nombre de termes de la serie $V + \delta V_1 + \delta^2 V_2 +$ etc., on aurait en général

$$\varphi(x) = \left\{ \begin{array}{l} A \cos a_1 \cos a_2 \cos a_3 \ldots \cos a_n \,.\, \sin b_1 \sin b_2 \ldots \sin b_m \\ + A_1 \cos c_1 \cos c_2 \cos c_3 \ldots \cos c_p \,.\, \sin d_1 \sin d_2 \ldots \sin d_r \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{etc.} \end{array} \right\};$$

pour opérer les réductions nécessaires dans cette formule on pourra faire usage de l'équation

$$\cos a_1 \cos a_2 \cos a_3 \ldots \cos a_n$$

$$= \frac{1}{2^{n-1}} \left(\cos q + S. \cos (q - 2 a_y) + S.S. \cos (q - 2 a_y - 2 a_z) \ldots + \text{etc.} \right),$$

dans laquelle les arcs $a_1, a_2, a_3, \ldots a_n$, sont indéterminés et tous différens entre eux, et donnent $a_1 + a_2 + a_3 \ldots + a_r = q$; en indiquant par $S. \cos (q - 2 a_y)$, la somme de tous les termes de la forme $\cos (q - 2 a_y)$, où l'on a fait successivement $y = 1, 2, 3, \ldots n$: en représentant par $S.S. \cos (q - 2 a_y - 2 a_z)$, la somme de tous les termes de la forme $\cos (q - 2 a_y - 2 a_z)$, où l'on a fait d'abord successivement $y = 1, 2, 3, \ldots n$; et où l'ou a donné à z toutes les valeur $1, 2, 3, \ldots n$; (pourvu que l'on néglige tous les termes dans lesquels on aurait $y = z$) et ainsi de suite jusqu'au dernier terme: en observant toujours d'omettre tous les termes de cette formule, qui seraient égaux à l'un de ceux que l'on a déjà trouvés. En différentiant cette équation par rapport à a_1, a_2, a_3, etc., on obtiendrait des expressions semblables, pour le produit d'un nombre quelconque de sinus et de cosinus.

M. Fourier en adoptant la loi de Newton a trouvé, que la demi-somme des températures de deux points de l'armille situés aux extrémités d'un diamètre quelconque, forme toujours, au bout d'un temps très-long, une quantité constante, et égale à la température moyenne de l'armille. Maintenant, puisque ce résultat à été confirmé par l'expérience, il est clair qu'il devra se déduire encore de la loi du refroidissement découverte par MM. Dulong et Petit. En effet, en reprenant la valeur de v trouvée précédemment (11), et en y supposant

t très-grand, on devra considérer seulemeot deux espèces de termes: ceux dans lesquels on a $s=0$, et ceux qui résultent de $s=1$: c'est-à-dire les termes multipliés par e^{-bt}, et par $e^{-\left(b+\frac{a}{r^2}\right)t}$; puisque tous les autres qui contieooent quelques-uns des facteurs $e^{-2\left(b+a\frac{m^2}{r^2}\right)t}$; $e^{-\left(b+4\frac{a}{r^2}\right)t}$ etc.; sont trop petits (dans l'hypothèse de t très-grand) pour être comparés à ceux-ci. Alors la valeur de v se réduira à la forme

$$v=B_0\,e^{-bt}+A_1\,e^{-\left(b+\frac{a}{r^2}\right)t}\sin\frac{x}{r}+B_1\,e^{-\left(b+\frac{a}{r^2}\right)t}\cos\frac{x}{r},$$

et il est clair que si dans cette équation on substitue $x+r\pi$, au lieu de x, on aura la température v_1, du point de l'armille diamétralement opposé à celui dont la distance à l'origine est x, exprimée de cette manière

$$v_1=B_0\,e^{-bt}-A_1\,e^{-\left(b+\frac{a}{r^2}\right)t}\sin\frac{x}{r}-B_1\,e^{-\left(b+\frac{a}{r^2}\right)t}\cos\frac{x}{r};$$

et partant

$$\frac{v+v_1'}{2}=B_0\,e^{-bt}.$$

Si dans la formule (11) on substitue pour b sa valeur $c\delta$, on trouvera, que l'expression de M. Fourier contient seulement la première puissance de δ, et que la nôtre renferme aussi δ^2. Avec notre méthode, on pourra pousser l'approximation aussi loin que l'on voudra, sans crainte de rencootrer jamais des arcs de cercle qui la reodraient nulle; et on pourra toojours déterminer les coostantes arbitraires (que l'on trouve en prenant des integrales particulières des premières équatioos différeotielles, pour les substitoer dans celles qui suivent) de manière que tous les termes aillent toojours en décroissant, et qu'aucun dénominateur ne s'évanouisse; comme nous l'avons fait dans l'analyse précédente.

On sait que l'équilibre des températures dans une armille, dont un point est soumis a une température constante, est donné lorsqu'on adopte la loi de Newton, par l'équation

$$\frac{d^2v}{dx^2} = n^2 v ;$$

dont l'integrale est $v = A e^{nx} + A_1 e^{-nx}$, A et A_1 étant deux constantes arbitraires. En partant de la loi de M. Dulong on obtient, pour l'équilibre des températures dans le vide, l'équation

$$\frac{d^2v}{dx^2} = a\left(e^{\delta v} - 1\right)$$

qui a pour intégrale

$$x = \int \frac{dv}{\sqrt{2a\left(\frac{e^{\delta v}}{\delta} - v\right) + C - \frac{2a}{\delta}}} + C_1 ;$$

C et C_1 étant deux nouvelles constantes arbitraires. Lorsque v est une petite quantité, on peut supposer sans erreur sensible

$$x = \int \frac{dv}{\sqrt{C + a\delta v^2}} + C_1 = \frac{1}{\sqrt{a\delta}} \log\left(v\sqrt{\frac{a\delta}{C}} + \sqrt{1 + \frac{a\delta v^2}{C}}\right) + C_1 ,$$

et en faisant $C_1 \sqrt{a\delta} = \log E$; $a\delta = n^2$; et réduisant, on aura

$$\left(\frac{e^{nx}}{E} - \frac{nv}{\sqrt{C}}\right)^2 = 1 + \frac{n^2v^2}{C} = \frac{e^{2nx}}{E^2} - \frac{2nve^{nx}}{E\sqrt{C}} + \frac{n^2v^2}{C} ,$$

et par suite

$$v = \frac{e^{nx}\sqrt{C}}{2nE} - \frac{E\sqrt{C}}{2ne^{nx}} = A e^{nx} + A_1 e^{-nx} ;$$

en faisant $A = \frac{\sqrt{C}}{2nE}$; $A_1 = -\frac{E\sqrt{C}}{2n}$; et comme v est égal à la température t du point que l'on considère, moins la température T de l'enceinte, on obtiendra enfin l'équation

$$t = A\, e^{nx} + A_1\, e^{-nx} + T ;$$

qui dans le cas de $T = 0$, coïncide avec celle que nous avions déjà trouvée, en supposant le refroidissement proportionnel à la différence des températures.

Si l'on considère une barre indéfinie très-mince, et que l'on suppose un foyer de température constante placé sur cette barre à l'origine des coordonnées, lorsque l'équilibre des températures se sera établi, cet état sera représenté par l'équation $\frac{d^2v}{dx^2} = n^2v$, pourvu que la température v soit assez petite pour pouvoir négliger, dans le développement de $e^{\delta v}$, les puissances de δv supérieures à la première : maintenant on sait que l'intégrale de l'équation précédente est $v = C\, e^{nx} + C_1\, e^{-nx}$; mais comme d'ailleurs l'état permanent de la barre est exprimé depuis $x = -\infty$, jusqu'à $x = +\infty$, par l'équation

$$v = C_2 \left(\frac{2}{\pi} \int_0^\infty \frac{dq \cos qx}{1 + q^2} \right)^n ,$$

et que quelque valeur que l'on attribue aux constantes, ces deux expressions de v ne peuvent jamais coïncider, il en résulterait que l'intégrale de l'équation $\frac{d^2v}{dx^2} = n^2v$, qui est linéaire, pourrait se former de la somme des deux valeurs de v que nous venons de rapporter, et contiendrait trois constantes arbitraires. Pour expliquer ce paradoxe il est nécessaire d'observer que l'équation $\frac{d^2v}{dx^2} = n^2v$, n'exprime l'état permanent de la barre, que dans les points qui permettent un flux de chaleur du point qui précède immédiatement celui que l'on considère, à celui-ci, et de celui-ci, à l'autre qui le suit immédiatement; tandis que le foyer, que nous avons placé à l'origine des coordonnées, envoye un flux continuel de chaleur à tous les points de la barre qui sont situés à sa droite et à sa gauche. Le même résultat se déduirait de la considération de la figure, qui

exprime les valeurs des températures pour chaque point de la barre, et dont l'équation est

$$y = C_2 \left(\frac{2}{\pi} \int_0^\infty \frac{dq \cos qx}{1+q^2} \right)^n ;$$

car pour $x = 0$, au lieu de donner $\frac{d^2y}{dx^2} = n^2 C_2$, comme cette courbe devrait faire si elle satisfaisait dans tous ses points à l'équation $\frac{d^2y}{dx^2} = n^2 y$, on voit, par la construction, qu'elle donne $\frac{d^2y}{dx^2} = \infty$; puisque la courbe dont nous parlons est formée de deux demi-logarithmiques égales, qui se réunissent de manière à avoir leur tangente commune au point de contact, perpendiculaire à l'axe des abscisses. Les mêmes considérations s'appliquent à une barre dont plusieurs points sont entretenus à des températures constantes: elle sont très-simples, mais nous avons cru devoir les placer ici, comme étant propres à limiter l'étendue que l'on serait tenté d'attribuer aux équations différentielles du mouvement de la chaleur, ou à leurs intégrales. Il faudra surtout y avoir égard, lorsqu'on voudra connaître l'état calorifique d'un corps, dont un ou plusieurs points pris dans son intérieur ou à sa surface, sont supposés des foyers de températures invariables.

Une autre observation que nous croyons ne pas devoir omettre, c'est que lorsque dans l'armille circulaire, que nous avons considérée, nous sommes partis de la propriété connue, que la température du point x devait être égale à celle du point dont la distance à l'origine est $x + 2r\pi$, pour déterminer la forme des fonctions circulaires comprises dans l'intégrale, nous l'avons fait en suivant l'exemple des illustres géomètres qui nous ont précédé dans ce genre de recherches. Cependant il paraît, qu'au lieu de partir de cette considération auxiliaire, on aurait dû déterminer les coefficiens de l'arc x d'après l'équation qui exprime la figure de l'armille, et l'irradiation qui se fait intérieurement entre les diverses parties de l'anneau; irradiation qui est modifiée, comme l'on sait, d'après la courbure intérieure de l'armille. Ceci deviendrait surtout évident, si l'on devait déterminer le mouvement de la chaleur sur une surface cylindrique creuse.

Enfin il faut remarquer, que la théorie mathématique de la chaleur a pour

but de trouver à chaque instant la température d'un point quelconque, d'après les conditions initiales du problème et la figure du corps que l'on considère. Cependant, dans la solution de ce problème, on suppose toujours que les coordonnées du point en question n'ont point changé, pendant que le corps s'est échauffé ou refroidi; quoiqu'il soit certain que ce point a changé de position, d'après l'augmentation ou la diminution de volume que le corps a soufferte par l'action de la chaleur. En opérant de cette manière on trouve la température d'une molécule matérielle, exprimée en fonction des coordonnées du point qu'elle occupait dans l'espace au commencement du phénomène, et du tems écoulé depuis la cessation de l'état initial: pour corriger les formules que l'on a obtenues, il faut connaître la loi d'après laquelle les corps se dilatent par l'effet de la chaleur. Si l'on suppose les dilatations linéaires élémentaires, proportionnelles aux accroissemens de la température, ce qui paraît toujours permis, du moins entre certaines limites de l'échelle thermométrique, on trouvera que le point qui, lorsque la température du corps était zéro, avait x pour distance à l'origine des coordonnées, sera éloigné de l'origine de la quantité $x_1 = \int dx\,(1 + \alpha v)$; v étant donné en fonction de x et de t; et le coefficient α étant donné dans chaque cas par l'expérience. Mais ceci n'est qu'un aperçu, que nous reprendrons dans une autre circonstance.

Ce mémoire est le même, à quelques changemens près, qui a été lu en 1825 à l'Académie Royale des Sciences de Paris.

MÉMOIRE

SUR LES FONCTIONS DISCONTINUES.

INTRODUCTION.

La question de la discontinuité des fonctions arbitraires, qui complètent les intégrales des équations aux différentielles partielles, agitée d'abord entre Daniel Bernoulli, Euler et d'Alembert, et discutée depuis par les plus grands géomètres, parait avoir été résolue par M. Fourier qui a montré le premier comment l'on pouvait déterminer, dans chaque cas particulier, les fonctions arbitraires de manière à satisfaire aux conditions initiales du problème, même lorsque celles-ci n'obéisseut pas aux lois de continuité. Les formules que cet illustre géomètre a trouvées sont propres à exprimer une fonction discontinue quelconque, dont les diverses parties, comprises entre des limites données de la variable, suivent une marche dissemblable, et sont représentées par des expressions différentes. Dans ces formules, les valeurs que la fonction doit prendre dans chaque cas et les conditions de discontinuité, sont combinées implicitement: cependant il nous a paru, que l'on pouvait toujours concevoir une fonction discontinue, comme étant égale à la somme d'un nombre donné de fonctions, chacune desquelles a une valeur continue entre deux limites connues, et qui s'évanouit hors de ces limites: dès-lors tout se réduit à trouver une fonction, qui donne une valeur constante entre deux limites données de la variable, et qui se réduise à zéro pour toutes les autres valeurs de la même variable; car en multipliant cette fonction, qui exprime la condition de discontinuité, par la fonction connue qui donne les valeurs que la formule doit prendre entre deux limites assignées, on aura l'expression cherchée entre les mêmes limites, et on parviendra à représeuter, par une somme d'expressions semblables, la valeur de la fonction discontinue pour des valeurs quelconques de la variable. Cependant on voit, que par cette méthode on obtiendrait pour les limites, des valeurs qui seraient égales à la somme de celles que l'on aurait, en

considérant ces limites comme appartenant successivement à chacune des fonctions qui viennent y aboutir.

En discutant les diverses valeurs que prennent quelques intégrales définies lorsqu'on fait varier les constantes qu'elles renferment, nous sommes aisément parvenus à trouver des formules, qui ont une valeur constante entre deux limites données et qui hors de ces limites s'évanouissent toujours. Ces formules cependant ne donnent pour les limites, que la moitié de la valeur constante qu'elles ont entre ces mêmes limites; de manière que si la fonction discontinue qu'il s'agit de représenter est un polygone on obtiendra, pour l'ordonnée de chaque sommet, la demi-somme des ordonnées qu'auraient dans ce point les deux côtés qui viennent s'y couper, et on trouvera dans ce cas seulement une valeur exacte aux limites. Mais on peut obtenir d'autres expressions dont la valeur soit toujours exacte aux limites, ou qui même devienne égale à une quantité quelconque; et nous montrons comment on peut les trouver.

Il résulte de là, que selon que pour exprimer les conditions de discontinuité, on aura fait usage d'une formule qui est exacte aux limites, ou d'une qui ne l'est pas, on obtiendra, après avoir multiplié par la fonction qui doit donner les valeurs, une formule qui représentera exactement la valeur de la fonction discontinue même aux limites, dans le premier cas, et qui ne sera pas exacte dans le second. Cela nous a fait soupçonner que comme, dans les formules que l'on avait trouvées en traitant les différens cas de la discontinuité des fonctions, on avait toujours réuni implicitement la fonction qui donne la valeur en général, à celle qui exprime la condition de discontinuité, sans discuter la valeur de celle-ci aux limites, et sans séparer en facteurs ces deux fonctions, il avait pu arriver dans quelques cas que l'on eût fait usage d'une formule de discontinuité qui ne fût pas exacte aux limites. En effet en cherchant à vérifier notre supposition sur quelques exemples de fonctions discontinues, discutées par les géomètres qui se sont occupés de la théorie de la chaleur, nous avons trouvé, pour quelques-unes de ces formules, la moitié de la valeur qu'elles devaient avoir aux limites: d'autres expressions, qui représentaient deux portions de courbe qui se coupent aux limites, nous ont donné pour ces points des valeurs exactes, comme cela devait arriver d'après notre analyse. Nous avons appliqué les mêmes considérations à quelques séries que l'on savait représenter des fonctions discontinues, et dans quelques cas nous avons trouvé aux limites la moitié de la valeur cherchée; mais dans d'autres exemples, ayant rencontré des valeurs qui

n'étaient pas la demi-somme de celles qu'avait la fonction très-près des limites, nous avons reconnu par là, que sans avoir discuté dans chaque formule la marche de la fonction qui exprime la condition de discontinuité, il est impossible d'assigner *à priori* d'une manière générale les valeurs des limites, et qu'il faut toujours les vérifier *à posteriori*.

Tout ce que nous venons de dire sur les valeurs que les fonctions discontinues prennent aux limites, tient spécialement à l'analyse pure; ces considérations seraient utiles dans les applications, si l'on pouvait supposer que les lois physiques restent les mêmes aux limites, lorsque les fonctions qui expriment les conditions initiales du problème changent brusquement de nature; mais cette hypothèse est peu vraisemblable, et n'est pas confirmée par les observations.

Toutes les formules que l'on avait trouvées jusqu'à présent, pour exprimer les fonctions discontinues, contenaient des séries infinies ou des intégrales définies, et l'on supposait qu'elles formaient une classe particulière de transcendantes: cependant en considérant les diverses valeurs des formules qui se présentent sous la forme $\frac{0}{0}$, on peut parvenir à représenter les fonctions discontinues en général, par des expressions qui ne contiennent que des fonctions logarithmiques et circulaires. Nous donnons pour exemple une de ces formules, et en l'appliquant à quelques cas particuliers, nous en déduisons des conséquences assez singulières. Ces expressions peuvent servir dans la détermination des valeurs des intégrales définies, et sont d'un grand usage dans la théorie des fonctions entières, comme nous espérons le montrer dans la suite de ces mémoires.

ANALYSE.

On sait que l'intégrale définie $A=\int_0^\infty \frac{dq}{q}\sin qx$ a pour valeur $\frac{\pi}{2}$, taut que x demeure positif et plus grand que zéro; et c'est dans ce sens qu'il faut entendre l'expression des géomètres, que la valeur de cette intégrale est indépendante de x; car lorsque $x=0$, on trouve $A=0$; et en faisant x négatif on obtient $A=-\frac{\pi}{2}$. Il résulte de là que l'intégrale définie

$$B=\int_0^\infty \frac{dq}{q}\sin bq\cos qx=\frac{1}{2}\int_0^\infty \frac{dq}{q}\sin(b+x)q+\frac{1}{2}\int_0^\infty \frac{dq}{q}\sin(b-x)q,$$

a pour valeur $\frac{\pi}{2}$ lorsque x a une valeur quelconque comprise entre $x=-b$, et $x=+b$; que pour $x=\pm b$, on trouve $B=\frac{\pi}{4}$; et que depuis $x=b$, jusqu'à $x=\infty$, et depuis $x=-b$, jusqu'à $x=-\infty$, on obtient $B=0$. On voit par conséquent que la formule

$$C=\frac{\pi}{2}+\int_0^\infty \frac{dq}{q}\sin qx\ ,$$

a pour valeur zéro, depuis $x=0$, jusqu'à $x=-\infty$; que pour $x=0$, elle donne $C=\frac{\pi}{2}$, et que pour toutes les valeurs positives de x, on a $C=\pi$. De même la formule

$$D=\int_0^\infty \frac{dq}{q}\sin bq\cos(x-a-b)q,$$

fournira $D=0$, depuis $x=a$, jusqu'à $x=-\infty$, et depuis $x=a+2b$, jusqu'à $x=\infty$; pour $x=a$, et pour $x=a+2b$, on obtiendra $D=\frac{\pi}{4}$; et

$D = \frac{\pi}{2}$, depuis $x=a$, jusqu'à $x=a+2b$. Maintenant si l'on multiplie l'intégrale D, par la fonction $\frac{2}{\pi}\varphi(x)$, on aura l'expression

$$E = \frac{2}{\pi}\varphi(x)\int_0^\infty \frac{dq}{q}\sin\frac{bq}{2}\cos\left(x-a-\frac{b}{2}\right)q\,,$$

qui aura pour valeur zéro, depuis $x=a$, jusqu'à $x=-\infty$, et depuis $x=a+b$, jusqu'à $x=\infty$: et qui depuis $x=a$, jusqu'à $x=a+b$, exprimera exactement la fonction $\varphi(x)$, excepté pour les deux limites $x=a$, $x=a+b$, pour lesquelles on aura $E=\frac{\varphi(a)}{2}$, $E=\frac{\varphi(a+b)}{2}$. En faisant les mêmes considérations sur la formule

$$\frac{2}{\pi}\varphi_1(x)\int_0^\infty \frac{dq}{q}\sin\frac{cq}{2}\cos\left(x-a-\frac{b}{2}-\frac{c}{2}\right)q,$$

on trouvera des résultats semblables; et pourtant l'expression

$$F = \frac{2}{\pi}\varphi(x)\int_0^\infty \frac{dq}{q}\sin\frac{bq}{2}\cos\left(x-a-\frac{b}{2}\right)q + \frac{2}{\pi}\varphi_1(x)\int_0^\infty \frac{dq}{q}\sin\frac{cq}{2}\cos\left(x-a-\frac{b}{2}-\frac{c}{2}\right)q$$

deviendra nulle depuis $x=a$, jusqu'à $x=-\infty$, et depuis $x=a+b+c$ jusqu'à $x=\infty$; et donnera $F=\frac{\varphi(a)}{2}$, pour $x=a$, et $F=\frac{\varphi_1(a+b+c)}{2}$ pour $x=a+b+c$; et $F=\frac{\varphi(a+b)+\varphi_1(a+b)}{2}$, pour $x=a+b$; et coïncidera avec la fonction $\varphi(x)$ depuis $x=a$, jusqu'à $x=a+b$; et avec la fonction $\varphi_1(x)$, depuis $x=a+b$, jusqu'à $x=a+b+c$.

Si les deux fonctions $\varphi(x)$, $\varphi_1(x)$, sont telles, qu'elles puissent représenter deux portions de deux courbes qui se coupent lorsque $x=a+b$, on aura pour le point d'intersection $\varphi(a+b)=\varphi_1(a+b)$; et pourtant la formule

F sera exacte même pour la valeur $x = a + b$, puisque dans ce cas $F = \frac{\varphi(a+b) + \varphi_1(a+b)}{2} = \varphi\,(a+b)$. L'on voit par là que les formules précédentes peuvent servir à représenter le contour d'un polygone dont les côtés sont des courbes quelconques: ce qu'on ne saurait faire si nos expressions donnaient pour les limites une valeur quelconque autre que $\frac{\varphi(a+b) + \varphi_1(a+b)}{2}$, puisque dans les polygones la loi de continuité venant à se rompre à chaque sommet, les formules que nous avons trouvées donnent pour tous ces points la demi-somme des deux ordonnées que l'on obtient en les considérant comme appartenant tantôt à l'un, tantôt à l'autre des deux côtés qui viennent s'y couper.

Si l'on voulait exprimer une fonction discontinue de x, qui donnât l'unité pour toutes les valeurs de x comprises entre $x = a$, $x = a + b$, sans excepter ces limites, et qui fût constamment égale à zéro pour toutes les autres valeurs réelles de x, on trouverait aisément la formule

$$\left\{\begin{array}{l} \frac{2}{\pi}\int_0^\infty \frac{dq}{q} \sin \frac{bq}{2} \cos\left(x - a - \frac{b}{2}\right)q \\ + \frac{4}{\pi^2}\left(\frac{\pi}{2} + \int_0^\infty \frac{dq}{q} \sin\,(x-a)q\right)\int_0^\infty \frac{dq}{q} \sin \frac{bq}{2} \cos\left(x - a - \frac{b}{2}\right)q \\ + \frac{4}{\pi^2}\left(\frac{\pi}{2} - \int_0^\infty \frac{dq}{q} \sin(x-a-b)q\right)\int_0^\infty \frac{dq}{q} \sin \frac{bq}{2} \cos\left(x - a - \frac{b}{2}\right)q \end{array}\right\}$$

$$= -2\left(\frac{2}{\pi}\int_0^\infty \frac{dq}{q} \sin \frac{bq}{2} \cos\left(x-a-\frac{b}{2}\right)q\right)^2 + \frac{3.2}{\pi}\int_0^\infty \frac{dq}{q} \sin \frac{bq}{2} \cos\left(x-a-\frac{b}{2}\right)q.$$

On peut parvenir directement au même résultat en observant que si

l'on indique par y l'intégrale définie

$$\frac{2}{\pi}\int_0^\infty \frac{dq}{q}\sin\frac{bq}{2}\cos\left(x-a-\frac{b}{2}\right)q,$$

le problème que nous venons de résoudre, se réduit à trouver une fonction de y telle que pour $y=1$, et pour $y=\frac{1}{2}$ elle donne $\varphi(y)=1$, et pour $y=0$ elle fournisse $\varphi(y)=0$; puisque 1, $\frac{1}{2}$ et 0, sont les trois valeurs de y; d'où l'on déduit.

$$\varphi(y)=-2(y-1)\left(y-\frac{1}{2}\right)+1=-2y^2+3y.$$

On peut trouver une infinité de formules propres à vérifier les conditions précédentes; mais on voit qu'elles conduiront toutes à des expressions du second degré, puisque il s'agit de trouver une équation qui ait deux racines. En général si l'on avait une fonction discontinue quelconque, qui eût seulement un nombre fini n de valeurs différentes dans une étendue finie ou infinie de la variable, il est clair que l'on pourrait, dans le même intervalle, la réduire à n'exprimer qu'une valeur constante donnée, à l'aide d'une équation du degré n qui aurait pour racines les diverses valeurs de la fonction connue. On pourrait même à l'aide de la théorie des équations, transformer une fonction discontinue, qui n'aurait qu'un nombre déterminé de valeurs, en une autre fonction discontinue de forme donnée quelconque; ce qui du reste ne saurait offrir aucune difficulté dans l'application.

Maintenant il résulte des considérations précédentes, que lorsque par les conditions d'un problème on sera conduit à une formule qui contiendra des fonctions discontinues, cette formule sera exacte aux limites, ou non, selon que l'on y sera parvenu à l'aide des expressions précédentes qui représentent exactement la fonction même aux limites, ou de celles qui ne donnent pour ces points, que la moitié des valeurs cherchées.

Pour appliquer ces réflexions à quelque cas particulier, nous considérerons le mouvement linéaire de la chaleur dans une barre infinie de très-petite épaisseur, en supposant que les températures initiales des points de la barre situés

entre $x = -1$, $x = +1$, aient pour valeur commune 1, et que tous les autres points depuis $x = -1$, jusqu'à $x = -\infty$, et depuis $x = 1$, jusqu'à $x = \infty$, soient à la température zéro. Les géomètres qui ont traité cette question, ont trouvé qu'en indiquant par t le tems écoulé depuis le commencement de l'observation, par v la température du point que l'on considère, et par x sa distance à l'origine des coordonnées, on avait l'équation

$$v = \frac{2e^{-bt}}{\pi} \int_0^\infty \frac{dq}{q} e^{-kq^2t} \cos qx \sin q ;$$

maintenant si l'on fait $t = 0$, dans cette formule, on devrait retrouver les températures initiales; mais par la discussion que nous avons faite précédemment de l'intégrale définie

$$\frac{2}{\pi} \int_0^\infty \frac{dq}{q} \sin q \cos qx ,$$

on trouve qu'elle satisfait aux conditions initiales du problème pour toutes les valeurs de x, excepté pour $x = \pm 1$; car pour ces valeurs elle donne $v = \frac{1}{2}$. Ainsi l'équation précédente n'exprime pas les conditions initiales, telles que nous les avions demandées; et correspond à un état initial qui donnerait $v = 0$, depuis $x = -1$, jusqu'à $x = -\infty$, et depuis $x = 1$, jusqu'à $x = \infty$; qui fournirait $v = \frac{1}{2}$ pour $x = \pm 1$; et $v = 1$, depuis $x = -1$, jusqu'à $x = 1$.

Pour représenter l'état des températures permanentes dans une barre échauffée par un foyer dont la température est 1, on a la formule

$$v = \frac{2}{\pi} \int_0^\infty \frac{dq \cos qx}{1 + q^2},$$

qui exprime deux courbes logarithmiques se coupant lorsque $x = 0$, à une distance égale à l'unité au dessus de l'axe des abscisses: maintenant comme au point d'intersection on a $e^0 = 1$, on sera dans le cas d'un polygone, et

l'équation sera exacte même pour les limites de chaque fonction; ce qui peut se vérifier aisément, puisqu'en faisant $x=0$, on a

$$v = \frac{2}{\pi}\int_0^\infty \frac{dq}{1+q^2} = \frac{2 \,.\, \pi}{\pi \,.\, 2} = 1 \,.$$

C'est peut-être par des considérations semblables, que l'on parviendrait à trouver *à priori* pourquoi la série

$$\left(\frac{1-\cos a}{1}\right)\sin x + \left(\frac{1-\cos 2a}{2}\right)\sin 2x + \left(\frac{1-\cos 3a}{3}\right)\sin 3x + \text{etc.}$$

(dont la somme est $\frac{\pi}{2}$ tant que l'on donne à x une valeur quelconque comprise entre 0 et a, et qui se réduit à zéro pour une valeur quelconque de x comprise entre a et π,) a pour valeur $\frac{\pi}{4}$ lorsqu'on fait $x=a=\frac{\pi}{2}$; ce qui est aisé à vérifier, puisqu'elle se réduit alors à

$$\left(1-\cos\frac{\pi}{2}\right)\sin\frac{\pi}{2} + \frac{1}{2}\left(1-\cos\frac{2\pi}{2}\right)\sin\frac{2\pi}{2} + \frac{1}{3}\left(1-\cos\frac{3\pi}{2}\right)\sin\frac{3\pi}{2} \ldots + \text{etc.}$$

$$= 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} \ldots \text{etc.} = \frac{\pi}{4}\,.$$

Tout ce que nous avons dit jusqu'ici nous paraît démontrer la nécessité de discuter dans chaque cas particulier la valeur des limites dans les fonctions discontinues, à moins que l'on ne connaisse par avance la nature de la formule d'où l'on a déduit les expressions qu'il s'agit de vérifier: car une formule qui exprime une fonction discontinue quelconque est le produit de deux facteurs, dont l'un représente l'équation à laquelle cette formule doit satisfaire entre deux limites données, et l'autre exprime la condition de la discontinuité; et on a vu que celle-ci peut être exacte ou non, aux limites. Si ces deux facteurs étaient toujours en évidence, il serait aisé dans tous les cas de vérifier les valeurs des limites; mais dans les formules auxquelles on parvient en résolvant les problèmes

qui comportent la discontinuité des fonctions, ces facteurs sont renfermés dans une expression commune, et on ne saurait les séparer. Par conséquent il faut dans chaque cas particulier discuter les valeurs des limites.

Les formules que nous avons trouvées précédemment, et qui mettent en évidence les facteurs dont nous venons de parler, sont utiles dans quelques cas pour faire connaître directement la marche de la fonction discontinue : on trouve par exemple

$$v = \frac{2}{\pi}\int_0^\infty \frac{dq \cos qx}{1+q^2} = \frac{e^{-x} + e^{x}}{2} + \left(\frac{e^{-x} - e^{x}}{\pi}\right)\int_0^\infty \frac{dq \sin qx}{q} \;;$$

et l'on voit que ces expressions serviraient de même a représenter l'état permanent d'une barre, dans laquelle il y aurait un nombre quelconque de foyers de température constante.

On pourrait aussi, par des formules semblables, exprimer des fonctions discontinues à deux ou à un plus grand nombre de variables: pourvu que l'on modifiât convenablement les conditions des limites.

Qu'il nous soit permis de remarquer ici, que l'on fairait disparaître quelques-unes des difficultés qui se rencontrent dans l'emploi des formules de transformation, dont on se sert pour l'intégration des équations aux différentielles partielles, et dans l'étendue qu'il faut attribuer aux fonctions arbitraires discontinues, si l'on faisait usage de la formule

$$\varphi(t) = \frac{1}{2\pi}\int_0^\pi \left\{ \frac{\varphi(x + e^{u\sqrt{-1}})}{1+(x-t)e^{-u\sqrt{-1}}} + \frac{\varphi(x+e^{-u\sqrt{-1}})}{1+(x-t)e^{u\sqrt{-1}}} \right\} du\,,$$

que nous avons donnée dans les Mémoires de l'Académie de Turin. Parceque la quantité x qui est indéterminée, et qui doit s'évanouir d'elle-même, sert à détruire les erreurs que l'on pourrait commettre en attribuant au développement de $\varphi(t)$ une forme qui ne lui conviendrait point. Du reste ces considérations, qui sont indispensables pour obtenir des résultats exacts, intéressent spécialement l'analyse des équations aux différentielles partielles qui expriment le mouvement de la chaleur, lorsqu'on suppose que les températures initiales

ne sont pas assujetties aux lois de continuité: car en considérant la question sous le rapport physique, il parait peu probable qu'aux limites de ces fonctions discontinues, la communication de la chaleur de molécule à molécule se fasse d'après la différence des températures.

Jusqu'à présent on n'a représenté les fonctions discontinues réelles, que par des suites infinies ou par des intégrales définies; et l'on ne connait aucune expression finie qui ne renferme que des quantités algébriques et des fonctions exponentielles ou circulaires, mais qui puisse cependant représenter une fonction discontinue. Toutefois en observant qu'en général, lorsque une fonction cesse d'obéir à la loi de continuité, on peut toujours supposer qu'elle passe par $\frac{o}{o}$ au point où elle change brusquement de nature, on parvient à trouver des formules qui ne contiennent que les transcendantes de l'algèbre élémentaire, et qui peuvent exprimer une fonction discontinue quelconque. Sans exposer les recherches qui nous ont conduit à ce résultat, et qui exigeraient de trop longs développemens, nous nous bornerons à vérifier *à posteriori* une de ces expressions, d'où l'on en pourra déduire une infinité d'autres.

Les géomètres qui se sont occupés de la détermination des valeurs particulières des coefficiens différentiels, ont reconnu depuis long-tems que la fonction $x^n \log x$, qui lorsque $x = o$ prend la forme $\frac{o}{o}$, se réduit à zéro pour cette valeur de x lorsque n est une quantité positive, et qu'elle devient infinie lorsque n est négative: maintenant si l'on discute les diverses valeurs de l'expression

$$e^{(\log y)e^{(\log y)(x-n)}}$$

lorsque $y = o$, ou ce qui revient au même de l'expression

$$z = e^{(\log o)e^{(\log o)(x-n)}},$$

on verra que lorsque x est une quantité positive quelconque plus grande que n, on aura $(x - n)\log o = -\infty$, et par conséquent

$$z = e^{(\log o)e^{-\infty}} = e^{-\infty e^{-\infty}} = e^{o} = 1:$$

mais comme on a, lorsque $x = n$,

$$\text{o} . \log \text{o} = \text{o},$$

on trouvera

$$e^{(\log \text{o}) e^{\text{o} . \log \text{o}}} = e^{(\log \text{o}) e^{\text{o}}} = e^{-\infty} = \text{o};$$

et enfin lorsque x est une quantité quelconque comprise entre n et l'infini négatif on aura $x - n = -p$, et par conséquent

$$(x - n) \log \text{o} = -p(-\infty) = \infty;$$

et partant

$$e^{(\log \text{o}) e^{(\log \text{o})(x-n)}} = e^{-\infty e^{\infty}} = e^{-\infty} = \text{o}.$$

D'où il résulte que la fonction

$$e^{(\log \text{o}) e^{(\log \text{o})(x-n)}}$$

est égale à zéro depuis $x = -\infty$, jusques et inclusivement à $x = n$, et que depuis $x = n$, jusqu'à $x = \infty$, cette fonction a pour valeur l'unité. Ainsi le produit

$$e^{(\log \text{o}) e^{(\log \text{o})(x-a)}} . e^{(\log \text{o}) e^{(\log \text{o})(a+b-x)}},$$

est nul pour toutes les valeurs de x comprises entre $x = a$ et $x = -\infty$; et entre $x = a + b$ et $x = \infty$; et est égal à l'unité pour toutes les valeurs de x comprises entre $x = a$ et $x = a + b$; excepté ces dernières limites pour lesquelles il se réduit à zéro. On peut observer que l'on a

$$e^{(\log \text{o}) e^{(\log \text{o})(x-a)}} = \text{o}^{\text{o}^{(x-a)}}.$$

Maintenant pour appliquer ces formules à un exemple nous chercherons, comme nous l'avons déjà fait, la formule qui exprime l'état permanent des températures dans une barre très-mince de longueur indéfinie, qui a un foyer de chaleur placé à l'origine des coordonnées et dont la température constante est égale à l'unité; et nous aurons

$$v = e^{x} \,.\, 0^{0^{-x}} + e^{-x} \,.\, \cos\frac{\pi}{2}\, 0^{0^{-x}}$$

d'où l'on déduit l'équation

$$\frac{2}{\pi}\int_{0}^{\infty}\frac{dq\cos qx}{1+q^{2}} = e^{x} \,.\, 0^{0^{-x}} + e^{-x} \,.\, \cos\frac{\pi}{2}\, 0^{0^{-x}}$$

qui donne la relation

$$\left\{e^{x} \,.\, 0^{0^{-x}} + e^{-x} \,.\, \cos\frac{\pi}{2}\, 0^{0^{-x}}\right\}^{n} = e^{nx} \,.\, 0^{0^{-x}} + e^{-nx} \,.\, \cos\frac{\pi}{2}\, 0^{0^{-x}}$$

On trouverait de la même manière l'expression d'un grand nombre d'intégrales définies dont on a cru jusqu'ici devoir former des classes distinctes de transcendantes, et qui ne sont que des formules contenant des fonctions logarithmiques et circulaires, dans lesquelles on a donné des valeurs particulières aux constantes qu'elles renferment. Nous montrerons dans la suite de ces recherches l'utilité de ces formules, dans la détermination des valeurs des intégrales définies, et les applications nombreuses qu'on en peut faire à la théorie des nombres, et en général à l'analyse des fonctions entières.

MÉMOIRE

SUR LA THÉORIE DES NOMBRES.

INTRODUCTION.

Les géomètres qui se sont occupés de l'analyse indéterminée, sont parvenus par leurs recherches plutôt à résoudre des questions spéciales, qu'à faire avancer l'ensemble de la science. Leurs méthodes, toujours bornées au problème qu'ils voulaient traiter, cessaient d'être utiles quand on tâchait de les appliquer à des questions plus étendues: bien plus, pour traiter un problème quelconque il fallait que les quantités connues fussent données en nombres; car sans cela, le manque absolu de formules générales empêchait de résoudre une équation indéterminée à coefficiens algébriques, même lorsqu'elle était du premier degré. De sorte que la théorie des nombres presqu'immobile au milieu des progrès des autres parties de l'analyse, qu'elle avait vu naître et s'élever successivement, s'en trouvait séparée et ne partageait pas leur perfectionnement commun. Cet isolement, qui forme la difficulté principale de la théorie des nombres, dépend de la méthode que l'on a suivie jusqu'ici pour mettre en équation les problèmes d'analyse indéterminée; car en exprimant seulement les relations qui doivent exister entre les valeurs des inconnues, on a toujours négligé de représenter par des signes algébriques les conditions auxquelles ces inconnues doivent satisfaire, afin qu'elles soient des nombres entiers ou rationnels. De sorte que ces conditions étant seulement sous-entendues, on ne peut pas les soumettre aux regles ordinaires de l'algèbre, et il en résulte un nouveau genre d'analyse, dont tout le succès dépend de la sagacité particulière de chacun des géomètres qui le cultivent, sans que les travaux des uns soient profitables aux recherches des autres. Il y a quelque tems que nous avons tâché de faire disparaître cette imperfection, et déjà nous avons montré ailleurs qu'en écrivant en analyse toutes les conditions du problème, les questions que l'on appelle indéterminées, deviennent toutes plus que déterminées, puisque l'on obtient toujours un nombre

d'équations qui surpasse de l'unité celui des inconnues. Nous reproduisons d'abord ici les formules que nous avons données dans cette occasion, pour exprimer par des séries convergentes le nombre ou la somme des racines d'une équation indéterminée, et nous y ajoutons de nouvelles expressions. Puis nous reprenons ce problème *à priori* dans toute sa généralité, et nous montrons comment, en partant des principes les plus élémentaires de l'analyse, on trouve pour chaque inconnue une équation algébrique dont le degré est égal à la limite que l'on attribue à l'inconnue, et qui exprime la condition que celle-ci doit être un nombre entier: de sorte qu'ayant de cette manière un nombre d'équations égal à celui des inconnues, en les combinant avec l'équation qui exprime les relations qui doivent exister entre les valeurs des variables, on aura après l'élimination une équation de condition qui ne contiendra que les coefficiens de l'équation proposée, et les limites qu'on aura attribuées aux inconnues. D'où il résulte que toute équation indéterminée, est réellement plus que déterminée. Ce résultat remarquable avait échappé à Euler qui croyait que les équations indéterminées devenaient plus que déterminées, seulement lorsque le nombre des formes que devaient prendre des fonctions données des variables, surpassait celui des inconnues. On explique par là, la contradiction qui se manifestait entre le nom d'équations indéterminées, et le fait qui montrait que souvent elles n'admettait pas de solutions: ce qui aurait dû faire soupçonner qu'il existait une équation de condition laquelle n'étant pas satisfaite, le problème ne pouvait pas être résolu. Et d'ailleurs en partant de la forme des racines des équations déterminées, et en observant que le nombre des solutions dans une équation indéterminée n'était pas donné par le degré de l'équation, on aurait pu prévoir que cette équation de condition était une fonction des coefficiens de l'équation proposée, et de la limite que l'on attribuait aux variables.

Les principes que nous exposons dans ce mémoire sont suffisans pour trouver, directement et sans tatonnement, toutes les solutions d'une équation indéterminée, lorsque la limite que l'on attribue aux variables n'est pas l'infini: mais comme le degré de l'équation de condition augmente avec les limites des inconnues; si l'on cherche toutes les solutions possibles d'une équation indéterminée, on trouvera une série infinie dont il s'agira d'avoir la somme pour résoudre la question proposée. Cette somme pourra s'exprimer par des intégrales définies, mais leur valeur numérique sera en général fort difficile à calculer; pour en faciliter la recherche il faudrait recourir à des principes que

nous n'avons pas cru devoir exposer dans ce mémoire, qui a pour but seulement de montrer en général l'esprit de notre méthode. Cependant pour qu'on ne puisse pas croire que notre théorie n'est pas susceptible d'être appliquée aux problèmes particuliers, et pour montrer de quelle manière nos formules peuvent se simplifier dans le plus grand nombre des cas, nous considérons spécialement dans ce mémoire les équations qui sont du premier degré par rapport à l'une des inconnues, et que M. Gauss a appellées congruences.

En donnant d'abord la théorie générale des congruences nous trouvons, que les relations existantes entre les coefficiens des équations algébriques et leurs racines, s'étendent aux congruences dont toutes les racines sont entières: nous démontrons de cette manière les théorèmes de Fermat et de Wilson, et beaucoup d'autres propositions nouvelles. Puis en appliquant aux congruences les principes qui renferment la théorie générale des équations indéterminées, on trouve les congruences de condition qui doivent être satisfaites afin que le problème soit résoluble: et ces conditions se simplifient beaucoup, à l'aide du théorème de Fermat, lorsque le module est un nombre premier.

En effectuant l'élimination entre les congruences, de la même manière que pour les équations, il devient facile d'obtenir le résultat final; et on trouve ainsi les relations qui doivent exister entre les coefficiens d'une congruence et le module, afin qu'elle soit résoluble. Ces relations, qui sont des congruences de condition, renferment toutes les conditions connues jusqu'à présent. Nous plaçons ici une courte digression sur les congruences à module variable, dans laquelle nous faisons voir qu'à l'aide de ces congruences on peut résoudre une classe assez étendue d'équations indéterminées, dont les plus simples avaient été traitées par Lagrange.

Pour chercher les conditions qui doivent être satisfaites afin qu'une congruence soit résoluble, au lieu de faire l'élimination à l'aide des coefficiens, on peut substituer les racines des congruences réduites à la forme d'équations déterminées: de cette manière on introduit les fonctions circulaires dans la théorie des congruences, et on trouve des formules qui la comprennent toute entière. Mais ces expressions ne sont pas assez simples pour qu'on puisse les appliquer avec facilité aux cas particuliers: par conséquent nous avons dû reprendre ce sujet d'une autre manière; et en partant d'une propriété très-simple de l'équation binome, nous avons trouvé des formules qui expriment le nombre et la somme des diviseurs d'un nombre quelconque, et nous avons formé deux intégrales

aux différences finies qui donnent le nombre et la somme des racines d'une congruence quelconque. Ces formules étant appliquées à la congruence du premier degré, fournissent l'expression générale de ses racines, qui sont une fonction trigonométrique des coefficiens et du module: et comme cette congruence équivaut à l'équation indéterminée du premier degré, on trouve ainsi les racines de cette équation en fonction de ses coefficiens, ce qui n'avait jamais été fait.

Nos formules générales étant appliquées aux congruences du second degré, donnent tous les théorèmes connus sur les résidus quadratiques: on en déduit aussi la manière de reconnaître *à priori* si un nombre quelconque est ou n'est pas résidu quadratique d'un nombre premier donné; et il en résulte une proposition générale qui renferme le théorème fondamental de M. Gauss.

La formule qui sert de base à notre théorie, et qui établit un rapport si singulier entre les solutions des congruences et les fonctions circulaires, fournit le moyen de résondre directement les équations à deux termes. M. Gauss qui a découvert le premier cette résolution par une méthode particulière, et Lagrange qui l'a ramenée ensuite à sa théorie générale des équations, ont supposé la connaissance des racines primitives. La théorie que nous exposons dans ce mémoire est indépendante de cette recherche, et d'ailleurs elle est beaucoup plus simple que les méthodes trouvées par ces deux grands géomètres, qui exigent de très-longs calculs pour être appliquées. On trouvera dans la suite de ces mémoires une méthode générale et très-simple pour traiter les équations de cette classe, de même que celles d'où dépend la division en parties égales de l'arc de la Lemniscate, et beaucoup d'autres; et l'on verra alors pourquoi la résolution de ces équations déterminées se réduit toujours à un problème d'analyse indéterminée.

En appliquant notre principe général aux congruences du troisième et du quatrième degré, nous avons trouvé des relations fort remarquables entre le nombre des solutions de certaines congruences, et les racines de quelques équations indéterminées du second degré. Nous avons tiré de là des considérations générales sur les résidus cubiques et bicarrés, sur lesquels on n'avait encore rien publié, en montrant comment l'on devait modifier les formes des nombres premiers qui servent de module, afin d'avoir des théorèmes généraux. On sait que pour avoir tous les théorèmes connus sur les résidus quadratiques d'un nombre premier, il suffit que la forme linéaire de ce nombre soit donnée. Mais cela est insuffisant pour les résidus cubiques et bicarrés, et il faut que le nombre

qui sert de module soit alors d'une forme quadratique donnée. Nous parvenons de cette manière à trouver la forme cubique des nombres premiers qu'on n'avait jamais considérée jusqu'à présent. On pourrait pousser plus loin l'examen des formes des degrés supérieurs, en observant que pour chaque degré le nombre des inconnues doit égaler ou surpasser l'exposant. La même chose arrive pour les congruences, et il est digne de remarque que quand on a déterminé le nombre des solutions d'une congruence, laquelle a autant d'inconnues qu'il y a d'unité dans l'exposant qui marque son degré, on aura tout de suite le nombre des solutions d'une autre congruence du même degré qui aurait le même module, mais qui contiendrait un plus grand nombre d'inconnues. C'est de cette considération que nous déduisons un théorème général sur les congruences de tous les degrés, qui renferme comme cas particulier un théorème de Lagrange sur les congruences du second degré à deux inconnues.

L'analyse succinte que nous venons de donner de notre mémoire suffit pour montrer la possibilité de déduire d'un seul principe général toute la théorie des nombres. Nous n'avons traité ici qu'une classe d'équations indéterminées: mais nous montrerons dans la suite comment on en peut résoudre un grand nombre d'autres, en appliquant le calcul d'approximation aux équations indéterminées, auxquelles il paraissait absolument inappliquable, mais qui cependant dans ce seul cas fournit des solutions exactes. Et nous fairons voir dans un mémoire particulier, comment l'on peut classer et discuter les transcendantes numériques, telles que les nombres premiers, les diviseurs des nombres, etc. En liant la théorie des nombres aux autres parties de l'analyse, il était certain que comme celles-ci contribueraient à son perfectionnement, elles en recevraient des secours; et c'est ce que nous montrerons dans la suite de ces recherches à l'égard des intégrales définies et des fonctions circulaires, dont plusieurs propriétés remarquables et inconnues jusqu'à présent, découlent de l'analyse indéterminée. Enfin nous fairons voir comment la considération des différens ordres d'irrationalité devient très-utile dans la résolution des équations numériques.

ANALYSE.

Nous avons montré pour la première fois, dans le 28.[e] Volume des Mémoires de l'Académie Royale des Sciences de Turin, qu'étant proposé de résoudre en nombres entiers l'équation

$$\varphi(x, y, z, \ldots\ldots \text{etc.}) = 0 ,$$

(que nous indiquerons pour abréger par $\varphi=0$) pour exprimer que x, y, z,... etc., doivent être des nombres entiers, on a les équations

$$\sin x\pi = 0 ; \quad \sin y\pi = 0 ; \quad \sin z\pi = 0 ; \ldots\ldots \text{etc.} ;$$

dont le nombre est égal à celui des inconnues, et qui doivent exister en même tems que l'équation proposée. Nous avons trouvé encore que le nombre des solutions entières et positives, plus grandes que zéro, de l'équation $\varphi=0$, est exprimé, à très-peu près par la formule

$$\sum_{x=1}^{x=\infty} \sum_{y=1}^{y=\infty} \sum_{z=1}^{z=\infty} \ldots\ldots\ldots e^{-10(x+y+z\ldots\ldots+\text{etc.})\varphi^2} .$$

S'il s'agissait d'exprimer le nombre des solutions entières de l'équation $\varphi=0$, en donnant à x, y, z, ... etc., toutes les valeurs $1, 2, 3, \ldots\ldots n-1$, on aurait la formule

$$(13) \ldots\ldots\ldots \sum_{x=1}^{x=n} \sum_{y=1}^{y=n} \sum_{z=1}^{z=n} \ldots\ldots\ldots e^{-10(x+y+z\ldots+\text{etc.})\varphi^2} =$$

$$\sum_{x=1}^{x=n} \sum_{y=1}^{y=n} \sum_{z=1}^{z=n} \ldots\ldots \left\{ \begin{array}{l} 1-10(x+y+z\ldots+\text{etc.})\varphi + \frac{100}{1.2}\overline{(x+y+z\ldots+\text{etc.})}^2\varphi^2 \ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \pm \frac{\overline{10}^a}{1.2.3\ldots a}\overline{(x+y+z\ldots+\text{etc.})}^a\varphi^a \mp \text{etc.} \end{array} \right\} .$$

On pourrait encore faire usage de la formule

$$\sum_{x=1}^{x=n}\sum_{y=1}^{y=n}\sum_{z=1}^{z=n}\ldots\ldots\frac{1}{1+(10x)^2\,(10y)^2\,(10z)^2\ldots\ldots\varphi^2};$$

et il serait facile de trouver plusieurs autres expressions semblables, propres à représenter le nombre ou la somme des solutions de l'équation proposée.

Le second membre de l'équation (13) est une série qui finira toujours par devenir convergente, et dont chaque terme pourra être calculé à l'aide des formules de la page 9. Mais pour avoir une valeur approchée du premier membre de l'équation (13) il faut calculer, dans le second membre, un nombre de termes qui augmente avec la limite n de l'intégration; de manière que l'on obtient toujours une expression de degré indéfini, qui est fonction des coefficiens de l'équation $\varphi = 0$, et de la limite n. Il faut remarquer surtout que les coefficiens des variables x, y, z, ... etc., dans le développement en série de l'intégrale qui forme le premier membre de l'équation (13), sont tels qu'en calculant un certain nombre de termes, il ne reste à peu près que ce qu'il faut pour donner le nombre des solutions de l'équation proposée. C'est de cette considération, et de l'examen attentif de la nature de ces coefficiens (qui s'expriment aussi par des intégrales définies) que l'on pourrait déduire des considérations qui jetteraient beaucoup de lumière sur la marche de la fonction représentée par la formule (13): mais ces recherches ne sauraient trouver place ici, et nous les exposerons dans un travail particulier.

Cet aperçu suffirait déjà pour montrer de quelle manière on pourrait réduire la théorie des nombres à l'analyse ordinaire: mais nous allons reprendre maintenant cette question dans toute sa généralité.

Etant proposée une équation à plusieurs inconnues à résoudre en nombres rationnels, fractionnaires ou entiers, on pourra toujours la préparer de manière que tous les nombres cherchés doivent être entiers et positifs: puisqu'en général, si l'équation proposée est de la forme

$$\varphi(x, y, z, \ldots \text{etc.}) = 0,$$

et que l'on cherche pour $x, y, z, \ldots$ etc., des valeurs fractionnaires, en faisant

$$x = \frac{x_1}{x_2}, \; y = \frac{y_1}{y_2}, \; z = \frac{z_1}{z_2}, \ldots \text{etc.},$$

on aura l'équation

$$\varphi\left(\frac{x_1}{x_2}, \frac{y_1}{y_2}, \frac{z_1}{z_2}, \ldots\ldots \text{etc.}\right) = 0,$$

dans laquelle il ne faudra chercher pour

$$x_1, \; x_2, \; y_1, \; y_2, \; z_1, \; z_2, \ldots\ldots \text{etc.},$$

que des valeurs entières: et d'ailleurs s'il y avait des solutions négatives on les obtiendrait en changeant les signes des variables. Nous supposerons par conséquent que ces réductions soient toujours effectuées dans les équations dont nous chercherons la résolution.

Soit proposé de résoudre en nombres entiers et positifs l'équation

$$\varphi(x, y, z, \ldots \text{etc.}) = 0,$$

que nous représenterons comme auparavant par $\varphi = 0$. Avec les méthodes connues on s'arrête là, et on tâche de résoudre cette équation en s'aidant de la forme particulière de ses coefficiens. Mais l'équation $\varphi = 0$, exprime seulement les relations qui doivent exister entre les inconnues, et n'indique pas que ces inconnues ne doivent recevoir que des valeurs entières et positives: pour exprimer cette dernière condition l'on supposera d'abord que l'on veuille trouver toutes les solutions qui s'obtiennent en donnant à x des valeurs moindres qu'une limite donnée a ; à y des valeurs plus petites que b ; à z des valeurs moindres que c ; et ainsi de suite: $a, b, c, \ldots$ etc., étant des nombres entiers et positifs. Il est clair qu'à cet effet l'on devra donner à $x, y, z, \ldots$ etc., toutes les

valeurs comprises dans les séries

$$\begin{array}{l} x = 0,\ 1,\ 2,\ 3,\ \ldots\ldots\ldots\ a-1\,; \\ y = 0,\ 1,\ 2,\ 3,\ \ldots\ldots\ldots\ b-1\,; \\ z = 0,\ 1,\ 2,\ 3,\ \ldots\ldots\ldots\ c-1\,; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{etc.}\,; \end{array}$$

et faire toutes les combinaisons possibles dans l'équation $\varphi = 0$. On observera que toutes ces valeurs de x se trouveront parmi les racines de l'équation

$$X = x\,(x-1)\,(x-2)\ldots\ldots\big(x-(a-1)\big) = 0\,;$$

et que de même les valeurs de y et de z seront comprises parmi les racines des équations

$$Y = y\,(y-1)\,(y-2)\ldots\ldots\big(y-(b-1)\big) = 0\,;$$

$$Z = z\,(z-1)\,(z-2)\ldots\ldots\big(z-(c-1)\big) = 0\,;$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{etc.}$$

Les équations précédentes expriment les conditions que x soit un nombre entier positif moindre que a; que y soit un nombre entier positif moindre que b; et ainsi de suite. Ces équations, dont le nombre est égal à celui des inconnues, étant combinées avec l'équation $\varphi = 0$, fournissent toutes les conditions du problème; de manière qu'ayant un nombre total d'équations qui surpasse de l'unité le nombre des inconnues, le problème sera plus que déterminé; et en éliminant successivement toutes les inconnues entre ces équations, on aura une autre équation de condition $F = 0$, qui comprendra les limites a, b, c, ... etc., assignées aux variables, et les coefficiens de l'équation proposée; et qui exprimera la relation qui doit exister entre ces quantités afin que le problème soit résoluble. Lorsque l'équation de condition sera satisfaite, et que l'on sera assuré que l'équation proposée peut être résolue, on reprendra l'une des équations à une seule inconnue que l'on a obtenues par l'élimination

avant de parvenir à l'équation $F=0$. Soit $X_1=0$, cette équation en x seul; en cherchant le plus grand diviseur commun entre $X=0$, et $X_1=0$, on aura une équation de la forme $X_2=0$, qui ne contiendra que l'inconnue x, et dont le degré sera égal au nombre des valeurs de x qui satisfont à l'équation proposée; et en résolvant l'équation $X_2=0$, on aura toutes les valeurs de x qui satisfont à l'équation $\varphi=0$. On pourrait trouver de même les valeurs des autres inconnues, qui résolvent l'équation proposée; et l'on voit que ce principe s'applique encore à la recherche directe des racines rationnelles d'une équation à une seule inconnue; car ce problème aussi dépend de la théorie des nombres.

Avec la méthode que nous venons d'indiquer, on a seulement les racines inégales; mais s'il y a des racines égales, elles peuvent se trouver avec facilité de la manière suivante. Nous supposerons d'abord, pour simplifier la question, qu'il s'agisse d'une équation à deux inconnues seulement; puisque la méthode est absolument la même lorsque le nombre des variables est plus grand.

Maintenant soit proposé de résoudre en nombres rationnels l'équation

$$\varphi(x, y)=0;$$

et supposons que n valeurs rationnelles de $x=a$, correspondent à une seule valeur rationnelle de $y=b$; (n étant un nombre plus grand que l'unité) en différentiant l'équation proposée par rapport à x, et cherchant le plus grand commun diviseur Δ, entre

$$\frac{d\,.\,\varphi(x, y)}{dx} \quad \text{et} \quad \varphi(x, y),$$

on aura $\Delta=F(x, y)$, et il y aura un reste $R=f(y)$ qui ne contiendra plus x, et qui par supposition devra se réduire à zéro. Si l'on fait par conséquent $f(y)=0$, on cherchera les racines rationnelles $y=b$, $y=b_1$, $y=b_2$, ... etc., de cette équation, lorsqu'il en existe, et en substituant successivement b, b_1, b_2, ... etc., pour y dans l'expression de Δ on aura les équations

$$F(x, b)=0\;;\; F(x, b_1)=0\;;\; F(x, b_2)=0\;;\;\ldots\ldots \text{etc.};$$

que l'on tâchera de réduire à la forme $(x-a)^{n-1}=0$; et on trouvera de cette manière les valeurs multiples de x que l'on cherche.

Si l'on avait identiquement $R=o$, on trouverait l'équation

$$\Delta = F(x,y) = \big(x - \psi(y)\big)^{n-1} = o,$$

qui devrait exister en même tems que l'équation $\varphi(x,y)=o$, et qui en serait un facteur: l'on ne pourrait donc pas déterminer de cette manière la valeur de $y=b$; mais en divisant le polynome $\varphi(x,y)=o$ par Δ, le quotient Q contiendrait une seule des n racines égales; et en cherchant le plus grand commun diviseur entre Δ et Q, on aurait l'équation $x-\psi(y)=o$. Nous avons supposé qu'il y avait seulement n valeurs de $x=a$, correspondantes à une valeur de $y=b$: mais si outre celles-là il y avait m valeurs de x égales à c, et r valeurs égales à e, etc., il serait facile d'appliquer encore à ce cas la méthode que nous venons d'exposer.

Soit proposée par exemple l'équation

$$x^2 - 2xy + 2y^3 - 1 = o,$$

dans laquelle on veuille savoir si parmi les valeurs rationnelles de y qui la résolvent il y en a une égale à b, et telle qu'il lui corresponde n valeurs de $x=a$; n étant un nombre plus grand que l'unité. A cet effet on différentiera l'équation proposée par rapport à x, et l'on aura $x-y=o$; puis en cherchant le plus grand commun diviseur entre ces deux équations, l'on trouvera $x-y$ pour ce diviseur et $2y^3-y^2-1=o$, pour reste, et comme cette dernière équation est satisfaite en faisant $y=1$, si l'on substitue cette valeur dans l'équation proposée, on aura

$$x^2 - 2x + 1 = (x-1)^2 = 1;$$

et par conséquent l'équation

$$x^2 - 2xy + 2y^3 - 1 = o,$$

est telle que deux valeurs de $x=1$, correspondent à la racine $y=1$.

On voit, par ce qui précède, quelles opérations il faudrait faire dans tous les cas; car si l'équation proposée contenait n inconnues, on la réduirait toujours à une autre qui en aurait $n-1$ seulement.

Maintenant il est clair que toute la théorie des nombres se ramène au problème de l'élimination; puisqu'il suffirait d'éliminer toutes les inconnues entre les équations

$$\varphi(x, y, z, \ldots \text{etc.}) = 0, \quad X = 0, \quad Y = 0, \quad Z = 0, \ldots \text{etc.},$$

que nous avons établies précédemment, pour trouver l'équation de condition $F = 0$, qui renferme la résolution de l'équation proposée. L'élimination générale entre ces équations ne saurait s'effectuer avec les méthodes connues; il est vrai que l'on pourrait substituer directement les valeurs des inconnues, mais il serait très-difficile de résoudre la question par cette voie. Pour la traiter avec quelque succès il faut recourir aux intégrales définies, et specialement aux integrales dont la valeur est indépendante des constantes qu'elles renferment. Mais nous nous réservons de donner cette théorie générale dans une autre occasion; et nous nous bornerons pour le moment à considérer les équations dans lesquelles l'une des inconnue est élevée seulement au premier degré, et que M. Gauss a nommées congruences; et nous déduirons d'une seule formule tout ce que l'on savait sur ce genre d'équations, et beaucoup d'autres résultats nouveaux. Cela nous fournira l'occasion de montrer un exemple des simplifications remarquables dont notre méthode est susceptible, lorsqu'on l'applique aux cas particuliers, et des artifices d'analyse dont il faut faire usage pour résoudre ce genre de questions.

Soit proposé de résoudre l'équation

$$(14) \ldots\ldots\ldots\ldots \varphi(x, y, z, \ldots \text{etc.}) \mp pu = 0;$$

dans laquelle φ exprime une fonction rationnelle et entière quelconque des nombres entiers $x, y, z, \ldots$ etc., et u doit être un nombre entier. Il est clair que s'il existe des valeurs de $x, y, z, \ldots$ etc., plus grandes que p, qui résolvent l'équation proposée, il y en aura aussi d'autres qui seront comprises entre zéro et p; et ce seront ces dernières que nous considérerons toujours dans ce qui suit, à moins que nous n'indiquions spécialement le contraire. A présent l'on sait que l'équation (14) équivaut, d'après la notation de M. Gauss, à la congruence

$$\varphi(x, y, z, \ldots \text{etc.}) \equiv 0 \ (\text{mod. } p).$$

En supposant, pour simplifier le problème, que cette congruence se réduise à la forme

$$X \equiv x^m + A_1 x^{m-1} + A_2 x^{m-2} \ldots\ldots + A_{m-1} x + A_m \equiv 0 \pmod{p},$$

(les coefficiens A_1, A_2, ... A_m étant toujours des nombres entiers) si elle a une racine entière $x = a_1$, on pourra toujours la mettre sous la forme $(x - a_1) X_1 \equiv 0 \pmod{p}$, X_1 étant un polynome entier en x du degré $m - 1$; il résulte de là que la congruence $X \equiv 0 \pmod{p}$ ne peut avoir, tout au plus, qu'un nombre m de racines entières moindres que p, m étant le nombre qui exprime le degré du polynome X ; et que si elle a les m racines entières

$$a_1, \quad a_2, \quad a_3, \ldots\ldots a_m,$$

on pourra faire

$$X \equiv (x - a_1)(x - a_2)(x - a_3) \ldots\ldots (x - a_m) \equiv 0 \pmod{p},$$

et on aura les congruences

$$(15)\ldots\left\{\begin{array}{l}
a_1 + a_2 + a_3 \ldots\ldots\ldots\ldots + a_m \equiv -A_1 \pmod{p},\\
\left.\begin{array}{l} a_1 a_2 + a_1 a_3 \ldots\ldots + a_1 a_m \\ + a_2 a_3 + a_2 a_4 \ldots\ldots + a_2 a_m \\ \ldots\ldots\ldots\ldots\ldots + \text{etc.}\end{array}\right\} \equiv A_2 \pmod{p},\\
\left.\begin{array}{l} a_1 a_2 a_3 + a_1 a_2 a_4 \ldots\ldots + a_1 a_2 a_m \\ + a_2 a_3 a_4 + a_2 a_3 a_5 \ldots\ldots + a_2 a_3 a_m \\ \ldots\ldots\ldots\ldots\ldots + \text{etc.}\end{array}\right\} \equiv -A_3 \pmod{p},\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
a_1 a_2 a_3 \ldots\ldots a_m \equiv \pm A_m. \pmod{p}.
\end{array}\right.$$

Dans cette dernière congruence il faudra prendre le signe $+$ si m est un nombre pair, et le signe $-$ si m est un nombre impair.

Pour trouver la somme des puissances r.^{mes} des racines de la congruence $X \equiv 0 \pmod{p}$, on aura des formules semblables à celles que l'on obtient pour les équations algébriques; car en appellant P_r, P_{r-1}, P_{r-2}, etc., la somme des puissances r.^{mes}, $(r-1)$.^{mes}, $(r-2)$.^{mes}, etc., de ces racines on aura

$$P_r + A_1 P_{r-1} + A_2 P_{r-2} \ldots\ldots + r A_r \equiv 0 \pmod{p}.$$

On peut de la même manière transformer les congruences et obtenir leurs fonctions symétriques. En général étant proposé de trouver une fonction symétrique donnée φ, des racines de la congruence $X \equiv 0 \pmod{p}$, qui a toutes ses racines entières, on cherchera la même fonction symétrique dans l'équation $X = 0$, et en exprimant dans l'équation la valeur de cette fonction par $\varphi = S$, on sera assuré que pour la congruence on aura

$$\varphi \equiv S \pmod{p}.$$

Soit maintenant proposé de résoudre la congruence

$$x^p - x \equiv 0 \pmod{p},$$

dans laquelle p est un nombre premier. Si l'on cherche une transformée en y dont les racines surpassent de l'unité celles de la proposée, on aura $y = x + 1$, et partant $x = y - 1$; d'où l'on déduira

$$(y-1)^p - (y-1) \equiv 0 \pmod{p}$$

et par suite, en négligeant les multiples de p,

$$y^p - y \equiv 0 \pmod{p}.$$

Mais comme cette dernière congruence est identique avec la proposée, il en résulte que celle-ci ayant la racine $x = a$, aura de même la racine $x = a + 1$, et par conséquent l'autre $x = a + 2$: et qu'en général elle sera résolue par

toutes les valeurs de x de la forme $a + z$; z étant un nombre entier positif quelconque: et puisque en faisant $x = 0$, on satisfait à la congruence proposée, elle aura pour racines tous les nombres naturels. Par conséquent la congruence

$$x^{p-1} - 1 \equiv 0 \ (\text{mod. } p),$$

aura pour racines tous les nombres $1, 2, 3, \ldots . p - 1$; ce qui forme le théorème de Fermat.

La congruence

$$x^{p-1} - 1 \equiv 0 \ (\text{mod. } p),$$

dans laquelle p est un nombre premier, étant comparée à l'autre

$$x^m + A_1 x^{m-1} + A_2 x^{m-2} \ldots . . + A_{m-1} x + A_m \equiv 0 \ (\text{mod. } p),$$

que nous avons déjà considérée, donne

$$A_1 = 0, A_2 = 0, \ldots . A_{m-1} = 0, A_m = -1;$$

$$m = p - 1; a_1 = 1, a_2 = 2, \ldots . a_m = p - 1;$$

et par conséquent, en substituant les valeurs des racines $a_1, a_2, a_3, \ldots . a_m$, dans les congruences (15), on aura

$$1 + 2 + 3 \ldots \ldots \ldots + p - 1 \equiv 0 \ (\text{mod } p),$$

$$\left. \begin{array}{l} 1 . 2 + 1 . 3 \ldots . . + 1 . (p-1) \\ + 2 . 3 + 2 . 4 \ldots . . + 2 . (p-1) \\ \ldots \ldots \ldots \ldots + \text{etc.} \end{array} \right\} \equiv 0 \ (\text{mod } p),$$

$$\ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \text{etc.},$$

et enfin

$$1 . 2 . 3 \ldots . . (p - 1) + 1 \equiv 0 \ (\text{mod } p),$$

puisque $p - 1$ est un nombre pair (*). Cette dernière congruence équivaut au théorème de Wilson.

Si l'on voulait trouver un nombre z tel qu'en faisant le produit de tous les nombres inférieurs à p (p étant un nombre premier) moins le facteur g, on eût

$$1 . 2 . 3 \ldots . (g-1)\ (g+1)\ \ldots . (p-1) + z \equiv 0 \ (\text{mod. } p),$$

on devrait chercher à déterminer les coefficiens de la congruence

$$x^{p-2} + \alpha\, x^{p-3} + \beta\, x^{p-4} \ldots\ldots + z \equiv 0 \ (\text{mod. } p),$$

qui a pour racines tous les nombres entiers inférieurs à p, excepté le nombre g: à cet effet on divisera la congruence

$$x^{p-1} - 1 \equiv 0 \ (\text{mod. } p)$$

par $x - g$, et le dernier terme du quotient sera le nombre z.

En effectuant la division l'on trouvera

$$\frac{x^{p-1}-1}{x-g} = x^{p-2} + g\,x^{p-3} + g^2\,x^{p-4} \ldots + g^{p-3}\,x + g^{p-2} + \frac{g^{p-1}-1}{x-g} \equiv 0 \ (\text{mod. } p),$$

et puisque $g^{p-1} - 1 \equiv 0$ (mod. p), on obtiendra

$$\frac{x^{p-1}-1}{x-g} \equiv x^{p-2} + g\,x^{p-3} \ldots\ldots\ldots + g^{p-3}\,x + g^{p-2} \equiv 0 \ (\text{mod. } p),$$

et partant

$$1 . 2 . 3 \ldots . (g-1)\ (g+1) \ldots . (p-2)\ (p-1) + g^{p-2} \equiv 0 \ (\text{mod. } p).$$

En faisant dans cette congruence $g = 1$, on retrouve le théorème de Wilson qui est un cas particulier de celui-ci.

(*) Si le nombre premier p était égal à 2, $p - 1$ ne serait plus un nombre pair; mais alors on aurait identiquement

$$1 + 1 \equiv 0 \ (\text{mod } 2).$$

On pourrait déduire de là tous les théorèmes que M. Gauss a insérés dans la troisième section de ses Recherches Arithmétiques, et beaucoup d'autres propositions nouvelles. Si l'on prend, par exemple, la somme des puissances n.^{mes} des racines de la congruence

$$x^{p-1} - 1 \equiv 0 \ (\text{mod.}\ p),$$

on trouve que, p étant un nombre premier, on aura toujours

$$1 + 2^n + 3^n \ldots\ldots + (p-1)^n \equiv 0 \ (\text{mod.}\ p),$$

lorsque n n'est pas divisible par $p-1$; tandis que si n est un multiple de $p-1$, on obtiendra

$$1 + 2^n + 3^n \ldots\ldots + (p-1)^n \equiv -1 \ (\text{mod.}\ p).$$

M. Poinsot a démontré que les racines de la congruence

$$x^n - 1 \equiv 0 \ (\text{mod.}\ np + 1),$$

dans laquelle $np + 1$ est un nombre premier, se déduisent des racines de l'équation $x^n - 1 = 0$, en ajoutant des multiples de $np + 1$ sous les radicaux compris dans l'expression de ces racines: mais cette proposition n'est qu'un cas particulier d'un théorème plus général que nous allons démontrer. En effet la congruence

$$x^n + A_1 x^{n-1} \ldots\ldots + A_{n-1} x + A_n \equiv 0 \ (\text{mod.}\ p),$$

dans laquelle p est un nombre quelconque, équivaut à l'équation à deux inconnues

$$x^n + A_1 x^{n-1} \ldots\ldots + A_{n-1} x + (A_n - py) = 0,$$

dont les racines sont exprimées par une formule de la forme

$$x = \varphi(A_1, A_2, \ldots\ldots A_{n-1}, A_n - py),$$

qui se réduit à l'expression des racines de l'équation

$$x^n + A_1 x^{n-1} \ldots\ldots + A_{n-1} x + A_n = 0,$$

lorsqu'on y fait $y = 0$. Si donc *vice versâ* l'on ajoute des multiples de p sous les radicaux compris dans l'expression des racines de cette équation, on aura les racines de la congruence proposée.

En appliquant aux congruences ce que nous avons dit en général des équations à plusieurs inconnues en nombres entiers, on trouve que toutes les solutions inégales et moindres que p de la congruence

$$\varphi(x, y, z, \ldots \text{etc.}) = \Phi \equiv 0 \pmod{p},$$

sont comprises parmi les racines des congruences

$$X = x(x-1)(x-2)\ldots\ldots\big(x-(p-1)\big) \equiv 0 \pmod{p},$$

$$Y = y(y-1)(y-2)\ldots\ldots\big(y-(p-1)\big) \equiv 0 \pmod{p},$$

$$Z = z(z-1)(z-2)\ldots\ldots\big(z-(p-1)\big) \equiv 0 \pmod{p},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{etc.};$$

et qu'en éliminant toutes les variables entre les congruences

$$\Phi \equiv 0 \pmod{p},\ X \equiv 0 \pmod{p},\ Y \equiv 0 \pmod{p},\ Z \equiv 0 \pmod{p}, \ldots \text{etc.},$$

on obtiendra une congruence de condition qui devra être satisfaite afin que la congruence proposée soit résoluble : de manière qu'au lieu d'avoir l'équation de condition $C = 0$, comme pour les équations, on aura la congruence de condition $C \equiv 0 \pmod{p}$, et l'expression qui aurait dû se réduire à zéro dans le premier cas, devra être divisible par p dans le second. Lorsque p est un nombre premier, la question se simplifie beaucoup, car par le théorème de Fermat on aura

$$x(x-1)(x-2)\ldots\ldots\big(x-(p-1)\big) \equiv x^p - x \equiv 0 \pmod{p},$$

$$y(y-1)(y-2)\ldots\ldots\big(y-(p-1)\big) \equiv y^p - y \equiv 0 \pmod{p},$$

$$z(z-1)(z-2)\ldots\ldots\big(z-(p-1)\big) \equiv z^p - z \equiv 0 \pmod{p},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{etc.},$$

et l'on devra éliminer les inconnues entre les congruences

$$\Psi \equiv o \,(\text{mod.}\, p),\, x^p - x \equiv o \,(\text{mod.}\, p),\, y^p - y \equiv o \,(\text{mod.}\, p),\, z^p - z \equiv o \,(\text{mod.}\, p), \ldots \text{etc.},$$

pour avoir la congruence de condition.

Si dans la congruence

$$\Psi \equiv o \;(\text{mod.}\, p)$$

on cherchait seulement les racines différentes de zéro, on devrait éliminer les inconnues entre cette congruence et les suivantes

$$x^{p-1} - 1 \equiv o \,(\text{mod.}\, p),\; y^{p-1} - 1 \equiv o \,(\text{mod.}\, p),\; z^{p-1} - 1 \equiv o \,(\text{mod.}\, p), \ldots \text{etc.},$$

et comme les racines congrues à zéro peuvent se trouver séparément avec facilité, nous supposerons, dans ce qui suit, que l'on cherche les racines différentes de zéro; ce qui simplifiera beaucoup nos recherches.

Il est clair, d'après ce que nous avons démontré sur les fonctions symétriques des congruences, qu'étant proposé d'éliminer les inconnues entre les congruences

$$\Phi \;=\; \varphi\,(x, y, z, \ldots\ldots \text{etc.}) \equiv o \quad (\text{mod.}\, p),$$
$$\Phi_1 \;=\; \varphi_1(x, y, z, \ldots\ldots \text{etc.}) \equiv o \quad (\text{mod.}\, p),$$
$$\Phi_2 \;=\; \varphi_2(x, y, z, \ldots\ldots \text{etc.}) \equiv o \quad (\text{mod.}\, p),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{etc.},$$

on pourra effectuer l'élimination entre les équations

$$\Phi = o\;,\quad \Phi_1 = o\;,\quad \Phi_2 = o\;,\; \ldots\ldots \text{etc.},$$

pourvu qu'au lieu de l'équation $F = o$, qui résultera de cette élimination, on écrive

$$F \equiv o \;(\text{mod.}\, p)\;.$$

Pour faire quelques applications de ce principe, soit proposé de résoudre

la congruence

$$Ax + B \equiv 0 \ (\text{mod. } p) \ ;$$

il est évident que si A et p ont un facteur commun, qui ne divise point B, cette congruence ne pourra pas se résoudre; et comme lorsque ce facteur commun existe et divise B, on peut toujours l'ôter, on pourra supposer que A et p sont premiers entre eux; et en faisant $x = Bz$, on aura

$$B\ (Az + 1) \equiv 0 \ (\text{mod. } p) \ ;$$

et il faudra résoudre la congruence

$$Az + 1 \equiv 0 \ (\text{mod. } p) \ .$$

Maintenant si l'on décompose p dans tous ses facteurs premiers, égaux ou inégaux, de manière que l'on ait

$$p = a.b.c \ldots\ldots n \ ,$$

on devra résoudre la congruence

$$Az + 1 \equiv 0 \ (\text{mod. } a.b.c \ldots\ldots n) \ ,$$

qui se change dans la suivante

$$Ay - 1 \equiv 0 \ (\text{mod. } a.b.c \ldots\ldots n) \ ,$$

en faisant $z = -y$.

En considérant la congruence

$$Ay - 1 \equiv 0 \ (\text{mod. } a) \ ,$$

il faudra éliminer entre celle-ci et la suivante $y^{a-1} - 1 \equiv 0 \ (\text{mod. } a)$, qui équivaut à l'autre

$$A^{a-1}\, y^{a-1} - 1 \equiv 0 \ (\text{mod. } a) \ ;$$

puisque par supposition a est un nombre premier qui ne divise point A: alors

en divisant $A^{a-1}y^{a-1}-1$, par $Ay-1$, on obtiendra un quotient exact; d'où l'on déduira que la congruence

$$Ay-1\equiv 0 \pmod{p},$$

est résolue en faisant

$$y=A^{a-2}s^{a-1}=Y_1\,;$$

en indiquant par s un nombre entier quelconque: on trouvera de même que toutes les congruences

$$Ay-1\equiv 0 \pmod{b}\ ,\ Ay-1\equiv 0 \pmod{c}, \ldots\ldots \text{etc.},$$

seront résolues en faisant successivement

$$y=A^{b-2}t^{b-1}=Y_2\ ;\ y=A^{c-2}u^{c-1}=Y_3\,;\ldots\ldots \text{etc.}$$

Il résulte de là que la congrueuce

$$(AY_1-1)(AY_2-1)(AY_3-1)\ldots\ldots\equiv 0 \pmod{a.b.c\ldots.n},$$

et par suite l'autre

$$Y=(AY_1-1)^2(AY_2-1)^2(AY_3-1)^2\ldots\ldots\equiv 0 \pmod{p},$$

seront toujours satisfaites: mais la valeur de y étant composée d'un nombre pair de facteurs, pourra se réduire à la forme

$$Az+1\equiv 0 \pmod{p}\,;$$

et puisque cette congruence est résoluble, l'autre

$$Ax+B\equiv 0 \pmod{p},$$

le sera de même, et on aura

$$x=\frac{B}{A}\left((A^{a-1}s^{a-1}-1)^2(A^{b-1}t^{b-1}-1)^2\ldots\ldots(A^{n-1}v^{n-1}-1)^2-1\right);$$



pour une de ses racines; en observant que l'on peut prendre pour s, t, ... v, des nombres entiers quelconques. En général toutes les solutions possibles de la congruence proposée seront données par la formule

$$x = \frac{B}{A}\Big((A^{a-1}-1)(A^{b-1}-1)\ldots.(A^{n-1}-1)\Big)^2 - \frac{B}{A} + pu,$$

dans laquelle u est un nombre entier quelconque.

Soit proposé maintenant de résoudre la congruence du second degré

$$x^2 + qx + r \equiv 0 \ (\text{mod. } 2p+1),$$

$2p+1$ étant un nombre premier; il est clair que si elle a une racine $x \equiv A$, il y en aura une autre $x \equiv B \equiv -q - A$, et partant si elle est résoluble il faudra qu'en divisant $x^{2p}-1$, par x^2+qx+r, le reste soit divisible par $2p+1$. A présent on doit remarquer que si α et β sont les deux racines de l'équation

$$x^2 + qx + r = 0,$$

on aura

$$x^2 + qx + r = (x-\alpha)(x-\beta),$$

et par conséquent

$$\frac{x^{2p}-1}{x^2+qx+r} = \frac{x^{2p}-1}{(x-\alpha)(x-\beta)} = \frac{x^{2p}-1}{(\beta-\alpha)(x-\beta)} + \frac{x^{2p}-1}{(\alpha-\beta)(x-\alpha)}:$$

en effectuant la division on trouvera le reste

$$\frac{1}{\beta-\alpha}\left(\frac{\beta^{2p}-1}{x-\beta}\right) + \frac{1}{\alpha-\beta}\left(\frac{\alpha^{2p}-1}{x-\alpha}\right),$$

qui devra être divisible par $2p+1$; ce qui donnera, en réduisant au même dénominateur,

$$\frac{1}{\beta-\alpha}\left(\frac{(x-\alpha)(\beta^{2p}-1)-(x-\beta)(\alpha^{2p}-1)}{(x-\alpha)(x-\beta)}\right) \equiv 0 \quad (\text{mod. } 2p+1),$$

et partant

$$\left(\frac{\beta^{2p}-\alpha^{2p}}{\beta-\alpha}\right)x-\alpha\beta\left(\frac{\beta^{2p-1}-\alpha^{2p-1}}{\beta-\alpha}\right)+\frac{\alpha-\beta}{\beta-\alpha}\equiv 0 \pmod{2p+1};$$

d'où l'on déduira les deux congruences de condition

$$(16)\ldots\ldots\ \frac{\beta^{2p}-\alpha^{2p}}{\beta-\alpha}\equiv 0 \pmod{2p+1}\ ;\ \alpha\beta\left(\frac{\beta^{2p-1}-\alpha^{2p-1}}{\beta-\alpha}\right)+1\equiv 0 \pmod{2p+1}.$$

On voit ici qu'après avoir effectué la division par $\beta-\alpha$, les premiers membres de ces deux congruences pourront toujours s'exprimer à l'aide des quantités q et r, puisqu'ils ne renferment que des fonctions symétriques des racines α et β : et d'ailleurs il est clair que l'on pourra toujours substituer au lieu de α et β, les quantités

$$\frac{-q+\sqrt{q^2-4r}}{2}\ ;\ \frac{-q-\sqrt{q^2-4r}}{2}\ .$$

Si dans la congruence

$$x^2+qx+r\equiv 0 \pmod{2p+1},$$

on fait $q=0$, $r=-s$; on devra dans les congruences (16) faire $\alpha+\beta=0$, et partant $\alpha=-\beta$; mais l'on a aussi $\beta=\sqrt{s}$, $\alpha=-\sqrt{s}$, $\beta-\alpha=2\sqrt{s}$, $\beta\alpha=-s$; par conséquent les deux congruences (16) se réduiront aux suivantes

$$\frac{\beta^{2p}-\beta^{2p}}{2\sqrt{s}}\equiv 0 \pmod{2p+1}\ ;\ -s\sqrt{s}\left(\frac{s^{p-1}+s^{p-1}}{2\sqrt{s}}\right)+1\equiv 0 \pmod{2p+1}\ ;$$

dont la première est toujours satisfaite, et la seconde se réduit à l'autre

$$(17)\ \ldots\ldots\ldots\ s^p-1\equiv 0 \pmod{2p+1}\ ;$$

qui est la condition déjà connue pour la résolution de la congruence

$$x^2 - s \equiv 0 \pmod{2p+1}.$$

Soit proposé, par exemple, de trouver la condition qui doit être satisfaite afin que la congruence $x^2 + 1 \equiv 0 \pmod{2p+1}$, dans laquelle $2p+1$ est un nombre premier, soit résoluble; on devra faire $s = -1$, dans la congruence de condition (17), et on aura

$$(-1)^p - 1 \equiv 0 \pmod{2p+1};$$

ce qui montre que p doit être un nombre pair.

En appliquant aux congruences du second degré les mêmes principes dont nous avons fait usage pour résoudre celles du premier degré, on pourrait trouver la résolution générale de la congruence

$$x^2 + qx + r \equiv 0 \pmod{p},$$

dans laquelle p est un nombre quelconque, pourvu que l'on connût tous les facteurs premiers de p.

En général étant proposée une congruence d'un degré quelconque

$$X = x^n + a_1 x^{n-1} + a_2 x^{n-2} \ldots\ldots + a_{n-1} x + a_n \equiv 0 \pmod{p},$$

dans laquelle p est un nombre premier, on divisera $x^{p-1} - 1$ par X (en faisant usage de la même méthode dont nous nous sommes servis pour les congruences du second degré) et on obtiendra un reste de la forme

$$X_1 = b_1 x^{n-1} + b_2 x^{n-2} \ldots\ldots + b_{n-1} x + b_n.$$

Maintenant si la congruence proposée a n racines entières, on devra avoir les n congruences de condition

$$b_1 \equiv 0 \pmod{p}, \quad b_2 \equiv 0 \pmod{p}, \ldots\ldots b_n \equiv 0 \pmod{p},$$

et on sera assuré que si elles sont satisfaites, la congruence $X \equiv 0 \pmod{p}$, aura toutes ses racines entières; mais si cette congruence n'avait qu'un nombre $n-m$ de racines entières, alors on devrait chercher de nouveau le plus grand commun diviseur entre X et X_1, et on trouverait enfin pour reste une

congruence de la forme

$$X_2 = c_1 x^{n-m-1} + c_2 x^{n-m-2} \ldots\ldots + c_{n-m} \equiv 0 \pmod{p},$$

qui donnerait les congruences de condition

$$c_1 \equiv 0 \pmod{p},\ c_2 \equiv 0 \pmod{p}, \ldots\ldots c_{n-m} \equiv 0 \pmod{p},$$

dont le nombre sera toujours égal au nombre des racines entières du la congruence proposée. On voit par là que la résolution d'une congruence du degré n, qui n'a que $n - m$ racines entières, se réduira à la résolution d'une congruence du degré $n - m$, en cherchant le plus grand commun diviseur entre X et $x^{p-1} - 1$.

Soit proposé, par exemple, de résoudre la congruence

$$x^a - b \equiv 0 \pmod{ap + 1},$$

dans laquelle $ap + 1$ est un nombre premier, on divisera $x^{ap} - 1$ par $x^a - b$, et on trouvera un quotient N et le reste $b^p - 1$; d'où il résulte que si la congruence

$$(18) \ldots\ldots\ldots\ldots \quad b^p - 1 \equiv 0 \pmod{ap + 1}$$

est résoluble, la congruence proposée aura toutes ses racines entières.

Les deux congruences de condition (17) et (18) avaient été trouvées par Fermat, mais avec sa méthode on ne pouvait pas trouver les conditions qui devaient être satisfaites, lorsque les congruences proposées n'étaient pas binomes: ce qu'on peut toujours effectuer par les principes que nous venons d'exposer.

La congruence de condition (18) montre que la congruence

$$x^3 - 1 \equiv 0 \pmod{6p + 1},$$

a toujours trois racines entières lorsque $6p + 1$ est un nombre premier; mais comme il est évident qu'une de ces racines est $x = 1$, on pourra diviser par $x - 1$, et on obtiendra la congruence du second degré

$$x^2 + x + 1 \equiv 0 \pmod{6p + 1},$$

qui aura ses deux racines entières: il faudra par conséquent que les deux

congruences (16) soient satisfaites quand on substitue pour α et β les deux racines de l'équation $x^2 + x + 1 = 0$, et que l'on change $2p + 1$ en $6p + 1$. Maintenant on a

$$\beta = -\frac{1}{2}(1 + \sqrt{-3}) \ ; \ \alpha = -\frac{1}{2}(1 - \sqrt{-3}) \ ;$$

et partant, la congruence $\frac{\beta^{6p} - \alpha^{6p}}{\beta - \alpha} \equiv 0 \pmod{6p + 1}$, deviendra la suivante

$$\frac{1}{2^{6p}\sqrt{-3}}\left((1 + \sqrt{-3})^{6p} - (1 - \sqrt{-3})^{6p}\right) \equiv 0 \pmod{6p + 1},$$

qui donnera en développant

$$\frac{1}{2^{6p}\sqrt{-3}}\left\{\begin{matrix} 1 + 6p\sqrt{-3} - \frac{6p(6p-1)}{2}.3 - \frac{6p(6p-1)(6p-2)}{2\,.\,3}.3\sqrt{-3} + \frac{6p(6p-1)(6p-2)(6p-3)}{2\,.\,3\,.\,4}.3^2 + \text{etc.} \\ -1 + 6p\sqrt{-3} + \frac{6p(6p-1)}{2}.3 - \frac{6p(6p-1)(6p-2)}{2\,.\,3}.3\sqrt{-3} - \frac{6p(6p-1)(6p-2)(6p-3)}{2\,.\,3\,.\,4}.3^2 + \text{etc.} \end{matrix}\right\}$$

$$= \frac{1}{2^{6p-1}}\left(6p - \frac{6p(6p-1)(6p-2)}{2\,.\,3}.3 + \frac{6p(6p-1)(6p-2)(6p-3)(6p-4)}{2\,.\,3\,.\,4\,.\,5}.3^2 - \text{etc.}\right) \equiv 0 \pmod{6p+1};$$

et par conséquent

$$(19)\ldots\ldots 6p - \frac{6p(6p-1)(6p-2)}{2\,.\,3}.3 + \frac{6p(6p-1)(6p-2)(6p-3)(6p-4)}{2\,.\,3\,.\,4\,.\,5}.3^2 - \text{etc.} \equiv 0 \pmod{6p + 1}.$$

Si l'on substitue les valeurs de α et β dans la congruence

$$\alpha\beta\left(\frac{\beta^{6p-1} - \alpha^{6p-1}}{\beta - \alpha}\right) + 1 \equiv 0 \pmod{6p + 1},$$

on aura, après avoir développé, la congruence

$$(20)\ldots(6p-1) - \frac{(6p-1)(6p-2)(6p-3)}{2\,.\,3}.3 + \frac{(6p-1)(6p-2)(6p-3)(6p-4)(6p-5)}{2\,.\,3\,.\,4\,.\,5}.3^2 - \text{etc.}\ldots - 2^{6p-2} \equiv 0 \pmod{6p + 1}.$$



Les deux congruences (19) et (20), que nous venons de trouver, et qui doivent toujours être satisfaites en même tems, lorsque $6p+1$ est un nombre premier, renferment un théorème exclusif et assez curieux, sur nombres premiers de la forme $6p+1$.

A présent si l'on effectue l'élimination de $6p$, entre la congruence

$$6p - \frac{6p(6p-1)(6p-2)}{2\,.\,3}\,.\,3 + \frac{6p(6p-1)(6p-2)(6p-3)(6p-4)}{2\,.\,3\,.\,4\,.\,5}\,.\,3^2 - \text{etc.} \equiv 0 \ (\text{mod. } 6p+1),$$

et l'autre, qni est toujours résoluble,

$$6p + 1 \equiv 0 \ (\text{mod. } 6p+1)$$

on trouvera, après les réductions,

$$-1 + \frac{1\,.\,2\,.\,3}{1\,.\,2\,.\,3}\,.\,3 - \frac{1\,.\,2\,.\,3\,.\,4\,.\,5}{1\,.\,2\,.\,3\,.\,4\,.\,5}\,.\,3^2 + \ldots\ldots \mp 3^{3p-1}$$

$$\equiv -1+3-3^2\ldots\ldots \mp 3^{3p-1} \equiv \frac{(-3)^{3p}-1}{4} \equiv (-3)^{3p}-1 \equiv 0 \, (\text{mod. } 6p+1).$$

Lorsque $p = 2n$, cette dernière congruence deviendra

$$3^{6n} - 1 \equiv 0 \ (\text{mod. } 12n+1),$$

et celle-ci sera toujours résoluble d'après ce qui précède: d'où il résulte, par la congruence de condition (17), que la congruence $x^2 - 3 \equiv 0 \, (\text{mod. } 12n+1)$ est toujours résolnble lorsque $12n+1$ est un nombre premier. On pourrait appliquer les mêmes principes à des congruences de degrés plus élevés, et on obtiendrait un grand nombre de théorèmes nouveaux, du même genre que ceux que nous venons d'énoncer; mais ces recherches nous écarteraient trop de notre but, et nous allons exposer de préférence quelques applications de la théorie des congruences à la résolutiou d'une classe d'équations indéterminées dont Lagrange a considéré les plus simples.

Soit proposé de résoudre en nombres entiers l'équation

$$y = \frac{a + a_1\,x + a_2\,x^2\,\ldots\ldots + a_n\,x^n}{e + e_1\,x + e_2\,x^2\,\ldots\ldots + e_m\,x^m} = \frac{X}{X_1};$$

on voit facilement que ce problème se réduit à la résolution de la congruence $X \equiv 0 \pmod{X_1}$; mais comme on a aussi identiquement $X_1 \equiv 0 \pmod{X_1}$, on pourra éliminer x entre ces deux congruences et on trouvera, après l'élimination, une congruence de condition $D \equiv 0 \pmod{X_1}$, dans laquelle D sera une fonction donnée des coefficiens

$$a\ ,\ a_1\ ,\ a_2\ ,\ \ldots\ldots a_n\ ;\ e\ ,\ e_1\ ,\ e_2\ ,\ \ldots\ldots e_m\ ;$$

et il faudra que X_1 divise le nombre D. Maintenant supposons que tous les diviseurs, positifs ou négatifs, de D soient représentés par la série des nombres

$$1\ ,\ d_1\ ,\ d_2\ ,\ d_3\ ,\ \ldots\ldots d_s\ ,\ D\ ;$$

on devra faire successivement

$$X_1 = 1\ ;\ X_1 = d_1\ ;\ X_1 = d_2\ ;\ \ldots X_1 = d_s\ ;\ X_1 = D\ ;$$

et en cherchant les racines entières de ces équations, on aura toutes les valeurs de x qui résolvent la congruence $X \equiv 0 \pmod{X_1}$, et par suite l'équation

$$y = \frac{a + a_1 x + a_2 x^2 \ldots\ldots + a_n x^n}{e + e_1 x + e_2 x^2 \ldots\ldots + e_m x^m} = \frac{X}{X_1}\,.$$

Etant donnée la même fraction $\frac{X}{X_1}$, on peut trouver aussi tous les nombres entiers qui, pour une même valeur de x, divisent à la fois le numérateur et le dénominateur. En effet si l'on représente en général par δ l'un de ces facteurs communs, on aura $X \equiv 0 \pmod{\delta}$; $X_1 \equiv 0 \pmod{\delta}$; et en éliminant x entre ces deux congruences (ou ce qui revient au même entre les deux équations $X = 0$, $X_1 = 0$,) on aura la congruence de condition $D \equiv 0 \pmod{\delta}$, et le nombre δ devra se trouver parmi les diviseurs de D. Il est clair que si X et X_1, avaient une racine commune α, il faudrait commencer par diviser ces deux polynomes par $x - \alpha$, autrement on aurait toujours $D = 0$.

Etant données les deux fonctions à deux inconnues $\varphi(x, y)$; $F(x, y)$; si elles ont un facteur commun δ on aura toujours

$$\varphi(x, y) \equiv 0 \pmod{\delta}\ ;\ F(x, y) \equiv 0 \pmod{\delta}\ ;$$

et en éliminant x ou y, entre ces deux congruences, on aura deux autres congruences de la forme

$$\Psi(x) \equiv 0 \pmod{\delta} \; ; \Psi_1(y) \equiv 0 \pmod{\delta}.$$

Soit proposé maintenant de résoudre en nombres entiers les deux équations simultanées

$$\varphi(x, y) = F(x, y) \cdot \psi(x, y, z) \; ; \; \Phi(x, y) = 0 \; ;$$

que nous exprimerons pour abréger par $\varphi = F \cdot \psi$; $\Phi = 0$; on pourra les réduire aux congruences

$$\varphi \equiv 0 \pmod{F} \; ; \; \Phi \equiv 0 \pmod{F} \; ; \; F \equiv 0 \pmod{F} \; ;$$

et en éliminant x et y entre ces trois congruences, on aura la congruence de condition

$$D \equiv 0 \pmod{F},$$

d'où l'on déduira toutes les valeurs possibles de F: l'on aura ainsi trois équations et trois inconnues, et les deux équations proposées seront résolues complètement.

Etant proposées les deux équations simultanées

$$\Phi(x, z) = \varphi(x, z) \cdot F(x, y, z) \; ; \; \Phi_1(x, z) = \varphi(x, z) \cdot F_1(x, y, z);$$

que nous indiquerons, pour abréger, par

$$\Phi = \varphi \cdot F \quad ; \quad \Phi_1 = \varphi \cdot F_1 \; ;$$

elles se transformeront dans les congruences

$$\Phi \equiv 0 \pmod{\varphi} \; ; \; \Phi_1 \equiv 0 \pmod{\varphi} \; ; \; \varphi \equiv 0 \pmod{\varphi} \; ;$$

d'où l'on déduira, par l'élimination, la congruence de condition $D \equiv 0 \pmod{\varphi}$, qui fournira toutes les valeurs possibles de φ; et l'on aura résolu complètement les deux équations proposées. On pourrait appliquer ces principes à des équations contenant un plus grand nombre d'inconnues; mais nous traiterons séparément cette matière dans un mémoire particulier sur les congruences à module variable.

En reprenant les congruences de condition, que nous avons données précédemment, il est clair que l'on pourra éliminer les inconnues entre la congruence à plusieurs inconnues

$$\varphi(x, y, z, \ldots \text{etc.}) \equiv 0 \pmod{p},$$

(dans laquelle p est un nombre premier) que nous indiquerons pour abréger par $\varphi \equiv 0 \pmod{p}$, et les suivantes

$$x^{p-1} - 1 \equiv 0 \pmod{p}\,;\; y^{p-1} - 1 \equiv 0 \pmod{p}\,;\; z^{p-1} - 1 \equiv 0 \pmod{p}\,; \ldots \text{etc.};$$

de la même manière que s'il s'agissait d'éliminer entre les équations

$$\varphi = 0 \;;\; x^{p-1} - 1 = 0 \;;\; y^{p-1} - 1 = 0 \;;\; z^{p-1} - 1 = 0 \;;\; \ldots \text{etc.} \;;$$

et que le résultat sera de la même forme: à présent pour éliminer les inconnues entre ces équations, on peut substituer dans la première toutes les valeurs de $x, y, z, \ldots$ etc., déduites des autres équations, et comme l'on a

$$x = 1 \;;\; x = \cos\frac{2\pi}{p-1} + \sqrt{-1}\sin\frac{2\pi}{p-1} \;;\; x = \cos\frac{4\pi}{p-1} + \sqrt{-1}\sin\frac{4\pi}{p-1} \;;$$

$$\ldots\ldots\ldots\ldots\ldots\; x = \cos\frac{2(p-2)\pi}{p-1} + \sqrt{-1}\sin\frac{2(p-2)\pi}{p-1} \,:$$

$$y = 1 \;;\; y = \cos\frac{2\pi}{p-1} + \sqrt{-1}\sin\frac{2\pi}{p-1} \;;\; y = \cos\frac{4\pi}{p-1} + \sqrt{-1}\sin\frac{4\pi}{p-1} \;;$$

$$\ldots\ldots\ldots\ldots\ldots\; y = \cos\frac{2(p-2)\pi}{p-1} + \sqrt{-1}\sin\frac{2(p-2)\pi}{p-1} \,:$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{etc.}:$$

en substituant l'une après l'autre toutes ces valeurs dans l'équation $\varphi = 0$, et faisant le produit de toutes les fonctions semblables que l'on obtiendra de cette manière, on trouvera la congruence de condition

$$e^{\sum_{x=0}^{x=p-1}\sum_{y=0}^{y=p-1}\sum_{z=0}^{z=p-1}\dots\log\varphi\left(\cos\frac{2x\pi}{p-1}+\sqrt{-1}\sin\frac{2x\pi}{p-1},\ \cos\frac{2y\pi}{p-1}+\sqrt{-1}\sin\frac{2y\pi}{p-1},\ \cos\frac{2z\pi}{p-1}+\sqrt{-1}\sin\frac{2z\pi}{p-1},\dots\text{etc.}\right)} \equiv 0 \ (\text{mod.}\ p).$$

Cette congruence parait assez singulière à cause des fonctions circulaires qu'elle renferme; cependant en observant le rapport qui existe entre la congruence $a \equiv a + px$ (mod. p), et l'équation $\cos\frac{a\pi}{p} = \cos\frac{(a+px)\pi}{p}$, lorsque a, p et x, sont des nombres entiers, on pourrait se rendre compte aisément de la forme de cette expression. On pourrait déduire de là plusieurs théorèmes connus sur les congruences; mais cette route serait longue et pénible, et nous préférons de partir d'une autre équation fondamentale qui servira à retrouver directement tout ce que l'on savait sur la théorie des congruences, et à découvrir beaucoup de propositions nouvelles. En observant que quoique par notre théorie on ne trouve que les racines inégales de la congruence $\varphi \equiv 0$, on obtiendra cependant les racines égales par la méthode dont nous avons fait usage pour les équations indéterminées; et même on les trouvera directement en éliminant entre les congruences

$$\varphi \equiv 0 \ (\text{mod.}\ p)\ ;\quad \frac{d\varphi}{dx} \equiv 0 \ (\text{mod.}\ p)\ ;\quad \frac{d\varphi}{dx} \equiv 0 \ (\text{mod.}\ p)\ ;\ \dots \text{etc.}$$

Etant donnée l'équation à une seule inconnue

$$x^m - 1 = 0,$$

si l'on représente par P_n, P_{n-m}, P_{n-2m}, ... etc., les sommes des puissances $n.^{\text{mes}}$, $(n-m).^{\text{mes}}$, $(n-2m).^{\text{mes}}$ .... etc., de ses racines, on aura

$$P_n = P_{n-m} = P_{n-2m} \dots\dots = P_{n-\nu m} = \text{etc.}\,;$$

de sorte que si n est un multiple de m, on obtient $P_n = m$; et dans le cas contraire on trouve $P_n = 0$. En exprimant les racines de l'équation $x^m - 1 = 0$, en fonctions circulaires, on aura

$$P_n = \begin{cases} \left(\cos\frac{0\pi}{m} + \sqrt{-1}\sin\frac{0\pi}{m}\right)^n + \left(\cos\frac{2\pi}{m} + \sqrt{-1}\sin\frac{2\pi}{m}\right)^n \ldots\ldots \\ + \left(\cos\frac{2u\pi}{m} + \sqrt{-1}\sin\frac{2u\pi}{m}\right)^n \ldots + \left(\cos\frac{2(m-1)\pi}{m} + \sqrt{-1}\sin\frac{2(m-1)\pi}{m}\right)^n. \end{cases}$$

Si l'on transforme la second membre au moyen de la relation connue

$$(\cos z + \sqrt{-1}\sin z)^n = \cos nz + \sqrt{-1}\sin nz,$$

et qu'on néglige les imaginaires qui, dans le cas actuel, doivent nécessairement se détruire, on obtiendra

$$(21) \ldots P_n = \cos\frac{0n\pi}{m} + \cos\frac{2n\pi}{m} + \cos\frac{4n\pi}{m} \ldots + \cos\frac{2un\pi}{m} \ldots + \cos\frac{2(m-1)n\pi}{m}$$

$$= \sum_{u=0}^{u=m} \cos\frac{2un\pi}{m} = \frac{\sin 2\left(n - \frac{n}{2m}\right)\pi + \sin\frac{n\pi}{m}}{2\sin\frac{n\pi}{m}};$$

et la valeur de cette expression sera m ou zéro, suivant que le nombre $\frac{n}{m}$ sera entier ou fractionnaire.

Il résulte de là que si l'on prend successivement la somme des puissances n.mes des équations

$$x - 1 = 0,\ x^2 - 1 = 0,\ x^3 - 1 = 0, \ldots\ldots x^m - 1 = 0,$$

on aura la somme des diviseurs de n, compris dans les nombres $1, 2, 3, \ldots m$;

et cette somme pourra être représentée par la formule

$$\sum_{x=1}^{x=m+1} \sum_{y=0}^{y=x} \cos \frac{2ny\pi}{x} = \sum_{x=1}^{x=m+1} \frac{\sin 2\left(n - \frac{n}{2x}\right)\pi + \sin \frac{n\pi}{x}}{2 \sin \frac{n\pi}{x}} .$$

On trouverait de même que le nombre des diviseurs de n, compris dans la série $1, 2, 3, \ldots m$, est donné par l'expression

$$\sum_{x=1}^{x=m+1} \sum_{y=0}^{y=x} \frac{1}{x} \cos \frac{2ny\pi}{x} = \sum_{x=1}^{x=m+1} \frac{\sin 2\left(n - \frac{n}{2x}\right)\pi + \sin \frac{n\pi}{x}}{2 \sin \frac{n\pi}{x}} .$$

Si l'on voulait exprimer la somme et le nombre de tous les diviseurs de n, en représentant par $\int(n)$ la première de ces fonctions, et par $\delta(n)$ la seconde, on aurait

$$\int(n) = \sum_{x=1}^{x=n+1} \sum_{y=0}^{y=x} \cos \frac{2ny\pi}{x} ,$$

$$\delta(n) = \sum_{x=1}^{x=n+1} \sum_{y=0}^{y=x} \frac{1}{x} \cos \frac{2ny\pi}{x} .$$

On sait que lorsque n est un nombre premier, on a

$$\int(n) = n + 1 \quad ; \quad \delta(n) = 2 ;$$

nous aurons donc, en changeant les limites des variables, les deux équations

$$\sum_{x=1}^{x=n} \sum_{y=0}^{y=x} \cos \frac{2ny\pi}{x} = 1 \quad ; \quad \sum_{x=1}^{x=n} \sum_{y=0}^{y=x} \frac{1}{x} \cos \frac{2ny\pi}{x} = 1 \; ;$$

qui renferment deux proprietés spéciales des nombres premiers.

On a vu que, n et m étant deux nombres entiers, la formule

$$\frac{\sin 2\left(n - \frac{n}{2m}\right)\pi + \sin \frac{n\pi}{m}}{2 \sin \frac{n\pi}{m}}$$

a pour valeur m, si n est divisible par m, et qu'elle se réduit à zéro lorsque cette condition n'est pas satisfaite. Nous avons démontré de plus, que p étant un nombre premier, l'expression

$$\frac{1 \cdot 2 \cdot 3 \ldots\ldots\ldots (p-1) + 1}{p}$$

ne peut devenir un nombre entier que lorsque p est un nombre premier; en faisant donc

$$m = p \,, \quad \text{et} \quad n = 1 \cdot 2 \cdot 3 \ldots\ldots (p-1) + 1 \,,$$

dans la formule (21), elle se transformera en celle-ci

$$\frac{\sin 2\left(1 \cdot 2 \cdot 3 \ldots (p-1) + \frac{1 \cdot 2 \cdot 3 \ldots\ldots (p-1)+1}{2p}\right)\pi + \sin\left(\frac{1 \cdot 2 \cdot 3 \ldots (p-1)+1}{2p}\right)\pi}{2 \sin\left(\frac{1 \cdot 2 \cdot 3 \ldots (p-1)+1}{2p}\right)\pi},$$

qui devient p lorsque p est un nombre premier, et qui se réduit à zéro dans le cas contraire. Ainsi cette formule représente exclusivement tous les nombres premiers. Si l'on voulait exprimer analytiquement la somme des nombres

premiers compris dans la série

$$a\,,\,a+1\,,\,a+2\,,\,\ldots\ldots\,a+b-1\,,$$

on aurait la formule

$$\sum_{x=a}^{x=a+b} \frac{\sin 2\left(1.2.3\ldots\ldots(x-1)+1-\frac{1.2.3\ldots(x-1)+1}{2x}\right)\pi+\sin\left(\frac{1.2.3\ldots(x-1)+1}{2x}\right)\pi}{2\sin\left(\frac{1.2.3\ldots(x-1)+1}{2x}\right)\pi}$$

On peut généraliser beaucoup ces expressions, et les appliquer aux séries périodiques, aux fonctions discontinues et à d'autres recherches: mais ce que nous en venons de dire suffit pour le moment.

Puisque la formule

$$\frac{1}{m}\left\{\begin{array}{l}\left(\cos\frac{0\,\pi}{m}+\sqrt{-1}\,\sin\frac{0\,\pi}{m}\right)^n+\left(\cos\frac{2\,\pi}{m}+\sqrt{-1}\,\sin\frac{2\,\pi}{m}\right)^n\ldots\ldots\\ \ldots\ldots\ldots+\left(\cos\frac{2(m-1)\pi}{m}+\sqrt{-1}\,\sin\frac{2(m-1)\pi}{m}\right)^n\end{array}\right\},$$

a pour valeur l'unité au zéro, suivant que $\frac{n}{m}$ est un nombre entier ou fractionnaire, il s'ensuit que le nombre N des racines inégales de la congruence à plusieurs inconnues

$$\varphi(x\,,y\,,z\,,\,\ldots\ldots\text{etc.})\equiv 0 \pmod{m},$$

(que nous exprimerons pour abréger par $\varphi\equiv 0 \pmod{m}$) dans laquelle on considère pour x, y, z, ... etc., les valeurs entières

$$\begin{array}{lllll} x=a & , a+1 & , a+2\,,\ldots\ldots\ldots & b & ; \\ y=c & , c+1 & , c+2\,,\ldots\ldots\ldots & d & ; \\ z=e & , e+1 & , e+2\,,\ldots\ldots\ldots & f & ; \end{array}$$

sera donné par l'équation

$$(22)\ldots\ldots\quad nN=\sum_{x=a}^{x=b}\sum_{y=c}^{y=d}\sum_{z=e}^{z=f}\ldots\left\{\begin{array}{l}\left(\cos\frac{0\,\phi\pi}{m}+\sqrt{-1}\sin\frac{0\,\phi\pi}{m}\right)+\left(\cos\frac{2\,\phi\pi}{m}+\sqrt{-1}\sin\frac{2\,\phi\pi}{m}\right)\ldots\ldots\\+\left(\cos\frac{2u\phi\pi}{m}+\sqrt{-1}\sin\frac{2u\phi\pi}{m}\right)\ldots+\left(\cos\frac{2(m-1)\phi\pi}{m}+\sqrt{-1}\sin\frac{2(m-1)\phi\pi}{m}\right)\end{array}\right\}$$

qui peut servir dans plusieurs cas à trouver la valeur de l'intégrale définie

$$\sum_{x=a}^{x=b}\ \sum_{y=c}^{y=d}\ \sum_{z=e}^{z=f}\ldots\ldots\cos\frac{a\phi(x\ ,\ y\ ,\ z\ ,\ldots\ldots\text{etc.})\pi}{m}\ ,$$

comme nous le montrerons dans la suite.

De même la somme des racines de la congruence $\phi\equiv 0\ (\text{mod. } m)$, comprises entre les mêmes limites que celles qui ont servi à déterminer la formule (22), sera donnée par l'intégrale

$$(23)\ldots\ \frac{1}{m}\sum_{x=a}^{x=b}\sum_{y=c}^{y=d}\sum_{z=e}^{z=f}\ldots(x+y+z\ldots+\text{etc.})\left\{\begin{array}{l}1+\left(\cos\frac{2\,\phi\pi}{m}+\sqrt{-1}\sin\frac{2\,\phi\pi}{m}\right)\ldots\ldots\\\ldots+\cos\left(\frac{2(m-1)\phi\pi}{m}+\sqrt{-1}\sin\frac{2(m-1)\phi\pi}{m}\right)\end{array}\right\}.$$

On pourrait trouver une infinité de formules du même genre; mais celles-ci suffisent déjà pour notre objet; et même elles sont trop générales, de manière qu'il faut les particulariser pour les appliquer avec facilité aux diverses questions que nous devrons résondre.

Nous observerons d'abord que, d'après ce que nous avons dit précédemment, il suffira d'intégrer entre les limites

$$0=x=y=z=\ldots\ldots\text{etc.}\ ,$$
$$m=x=y=z=\ldots\ldots\text{etc.}\ ,$$

pour savoir si la congruence proposée est ou n'est pas résoluble; et qu'ensuite les imaginaires devant se détruire entre eux, on pourra considérer l'intégrale

(24) .....

$$\frac{1}{m}\sum_{x=0}^{x=m}\sum_{y=0}^{y=m}\sum_{z=0}^{z=m}\ldots\left(1+\cos\frac{2\varphi\pi}{m}+\cos\frac{4\varphi\pi}{m}\ldots+\cos\frac{2u\varphi\pi}{m}\ldots\ldots+\cos\frac{2(m-1)\varphi\pi}{m}\right),$$

au lieu de celle fournie par l'équation (22), et l'intégrale

(25).....

$$\frac{1}{m}\sum_{x=0}^{x=m}\sum_{y=0}^{y=m}\sum_{z=0}^{z=m}\ldots(x+y+z\ldots+\text{etc.})\left(1+\cos\frac{2\varphi\pi}{m}+\cos\frac{4\varphi\pi}{m}\ldots+\cos\frac{2u\varphi\pi}{m}\ldots+\cos\frac{2(m-1)\varphi\pi}{m}\right),$$

à la place de la formule (23).

Soit proposé, par exemple, de trouver le nombre N des solutions entières, positives et moindres que c, de la congruence

$$ax+b\equiv 0 \pmod{c},$$

la formule (24) se changera, dans ce cas, dans la suivante

$$(26)\ldots\frac{1}{c}\sum_{x=0}^{x=c}\left(1+\cos 2(ax+b)\frac{\pi}{c}\ldots\ldots+\cos 2u(ax+b)\frac{\pi}{c}\ldots\ldots+\cos 2(c-1)(ax+b)\frac{\pi}{c}\right),$$

qui exprimera le nombre N cherché.

Si l'on considère le tems général de cette série, on aura l'équation

$$\frac{1}{c}\sum_{x=0}^{x=c}\cos 2u(ax+b)\frac{\pi}{c}=\frac{\sin 2u\left(b+ac-\frac{a}{2}\right)\frac{\pi}{c}-\sin 2u\left(b-\frac{a}{2}\right)\frac{\pi}{c}}{2c\sin\frac{ua\pi}{c}},$$

dans le second nombre de laquelle le numérateur est toujours zéro, mais dont

le dénominateur ne peut se réduire à zéro, que lorsque a et c ont un diviseur commun plus grand que l'unité, puisque u est toujours plus petit que c. Il résulte de là que si a et c sont premiers entre eux, tous les termes de la série (26) s'évanouissent, excepté le premier dont le valeur se réduit à

$$\frac{1}{c}\sum_{x=0}^{x=c} 1 = \frac{c}{c} = 1 \quad .$$

Mais si a et c ont un facteur commun g, on supposera $a = mg$; $c = ng$; et en faisant $u = n$, on obtiendra

$$\frac{1}{c}\sum_{x=0}^{x=c} \cos 2n(ax+b)\frac{\pi}{c} = \frac{\sin 2n\left(b+ac-\frac{a}{2}\right)\frac{\pi}{c} - \sin 2n\left(b-\frac{a}{2}\right)\frac{\pi}{c}}{2c \sin \frac{na\pi}{c}}$$

$$= \frac{\sin 2\left(b+ang-\frac{a}{2}\right)\frac{\pi}{g} - \sin 2\left(b-\frac{a}{2}\right)\frac{\pi}{g}}{2\,ng \sin \frac{a\pi}{g}} \, .$$

Cette expression se réduit à $\frac{0}{0}$, en vertu de l'hypothèse $a = mg$. On devra donc différentier le numérateur et le dénominateur par rapport à a, pour avoir une valeur déterminée, et l'on trouvera après les réductions

$$\frac{\sin 2\left(b+ang-\frac{a}{2}\right)\frac{\pi}{g} - \sin 2\left(b-\frac{a}{2}\right)\frac{\pi}{g}}{2\,ng \sin \frac{a\pi}{g}} = \cos \frac{2b\pi}{g} \, .$$

Si au lieu de prendre $u = n$, on fait en général $u = en$, e étant un nombre entier quelconque, on trouve

$$\frac{1}{c}\sum_{x=0}^{x=c} \cos en\,(ax+b)\frac{\pi}{c} = \cos \frac{2eb\pi}{g} \quad ;$$

et comme le nombre n est compris $g-1$ fois dans $c-1$, on pourra faire successivement $e=0, 1, 2, 3, \ldots. g-1$; et la valeur de l'intégrale (26) sera exprimée (dans le cas actuel où l'on suppose que a et c ont un commun diviseur g) par la série

$$1+\cos\frac{2b\pi}{g}+\cos\frac{4b\pi}{g}\ldots\ldots\ldots+\cos\frac{2(g-1)b\pi}{g},$$

dont la somme

$$\frac{\sin 2\left(b-\frac{b}{2g}\right)\pi+\sin\frac{b\pi}{g}}{2\sin\frac{b\pi}{g}},$$

a pour valeur g, lorsque $\frac{b}{g}$ est un nombre entier, et qui se réduit à zéro dans le cas contraire.

De là résulte

1.° Que la congruence $ax+b\equiv 0$ (mod. c), a toujours une solution entière et plus petite que c, lorsque a et c n'ont d'autres diviseurs communs que l'unité.

2.° Que si a et c ont un commun diviseur g différent de l'unité, qui ne divise point b, cette congruence n'admet aucun solution entière.

3.° Qu'enfin si $\frac{b}{g}$ est un nombre entier, on trouvera pour x un nombre g de valeurs entières plus petites que c, qui satisfont à la congruence proposée.

Maintenant si l'on fait $\varphi=ax+b$, et $m=c$, dans l'intégrale (25), on trouvera que la formule

$$(27)\ldots\ldots \sum_{x=0}^{x=c} x\left(1+\cos 2(ax+b)\frac{\pi}{c}\ldots.+\cos 2u(ax+b)\frac{\pi}{c}\ldots.+\cos 2(c-1)(ax+b)\frac{\pi}{c}\right),$$

exprimera la somme des valeurs de x, entières et moindres que c, qui satisfont à la congruence $ax+b=0$ (mod. c), lorsqu'elle est résoluble, et que

lorsqu'elle ne l'est pas, cette intégrale se réduit à zéro.

Nous avons démontré que si a et c ont un facteur commun différent de l'unité, et qui ne divise pas b, la congruence $ax+b\equiv 0$ (mod. c), n'admet aucune solution entière; et comme, si ce facteur commun divise aussi b, on peut toujours le supprimer, il sera permis, dans ce cas, de supposer que a et c sont premiers entre eux; et alors on sera assuré qu'il existe toujours une valeur entière de x, comprise entre zéro et c, qui satisfait à la congruence proposée; mais comme il n'existe qu'une seule de ces valeurs, comprise entre les limites que nous venons d'indiquer, la formule (27) qui exprime la somme des racines de la congruence

$$ax+b\equiv 0\ (\text{mod. } c)\,,$$

aura pour valeur la plus petite de ces racines entières et positives.

Actuellement pour trouver cette valeur de x, on considèrera le terme général de l'intégrale (27), et on aura

$$\frac{1}{c}\sum_{x=0}^{x=c} x\cos 2u(ax+b)\frac{\pi}{c}=\left\{\begin{array}{l}\dfrac{(c-1)\sin 2u\left(b+ca-\dfrac{a}{2}\right)\dfrac{\pi}{c}+\sin 2u\left(b-\dfrac{a}{2}\right)\dfrac{\pi}{c}}{2c\sin\dfrac{ua\pi}{c}}\\[2ex] +\dfrac{\cos 2u\left(ca+b-a\right)\dfrac{\pi}{c}-\cos 2u\left(b-a\right)\dfrac{\pi}{c}}{c\left(2\sin\dfrac{ua\pi}{c}\right)^2}\end{array}\right\},$$

où il faudra faire successivement $u=1,\ 2,\ 3,\ldots\ldots\ c-1$; et ajouter au résultat le premier terme de la série (27), qui est

$$\frac{1}{c}\sum_{x=0}^{x=c} x=\frac{c(c-1)}{2c}=\frac{c-1}{2}\,.$$

Puisque a et c, sont premiers entre eux, et que u est plus petit que c, il

s'ensuit que le dénominateur $2c \sin \frac{ua\pi}{c}$ ne pourra jamais s'évanouir ; on obtiendra par conséquent, en faisant les réductions nécessaires,

$$\frac{(c-1)\sin 2u\left(ac+b-\frac{a}{2}\right)\frac{\pi}{c}+\sin 2u\left(b-\frac{a}{2}\right)\frac{\pi}{c}}{2c\ \sin\ \frac{ua\pi}{c}}+\frac{\cos 2u\left(ac+b-a\right)\frac{\pi}{c}-\cos 2u\left(b-a\right)\frac{\pi}{c}}{c\left(2\ \sin\ \frac{ua\pi}{c}\right)^{2}}$$

$$=\frac{\sin\ 2u\left(b-\frac{a}{2}\right)\frac{\pi}{c}}{2\ \sin\ \frac{ua\pi}{c}}\ ;$$

et partant

$$(28)\ldots\ \frac{1}{c}\sum_{x=0}^{x=c}x\left(1+\cos 2(ax+b)\frac{\pi}{c}\ \ldots.+\cos 2u(ax+b)\frac{\pi}{c}\ \ldots.+\cos 2(c-1)(ax+b)\frac{\pi}{c}\right)$$

$$=\left\{\begin{array}{l}\frac{c-1}{2}+\frac{\sin 2\left(b-\frac{a}{2}\right)\frac{\pi}{c}}{2\sin\frac{a\pi}{c}}+\frac{\sin 4\left(b-\frac{a}{2}\right)\frac{\pi}{c}}{2\sin\frac{2a\pi}{c}}\ \ldots\ldots\ldots\ldots \\ +\frac{\sin 2u\left(b-\frac{a}{2}\right)\frac{\pi}{c}}{2\sin\frac{ua\pi}{c}}\ \ldots\ldots+\frac{\sin 2(c-1)\left(b-\frac{a}{2}\right)\frac{\pi}{c}}{2\sin(c-1)\frac{a\pi}{c}}\end{array}\right\}$$

$$=\frac{c-1}{2}+\frac{1}{2}\sum_{u=1}^{u=c}\frac{\sin\ 2u\left(b-\frac{a}{2}\right)\frac{\pi}{c}}{\sin\ \frac{ua\pi}{c}}=a\,.$$

Cette formule très-simple donne pour α la plus petite valeur de x qui satisfasse à la congruence $ax + b \equiv 0 \pmod{c}$, en nombres entiers et positifs : mais toutes les valeurs entières de x sont données, par l'équation

$$(29) \; \ldots \; x = \frac{c-1}{2} + \frac{1}{2} \sum_{u=1}^{u=c} \frac{\sin 2u\left(b - \frac{a}{2}\right)\frac{\pi}{c}}{\sin \frac{ua\pi}{c}} + cz ,$$

dans laquelle z est un nombre entier quelconque.

Il faut observer ici que la congruence

$$ax + b \equiv 0 \pmod{c} ,$$

équivaut à l'équation du premier degré à deux inconnues

$$ax + b = cy \;\; ;$$

et que la formule (29), donnera toutes les valeurs de x qui résolvent cette équation.

Soit proposé, par exemple, de résoudre en nombres entiers l'équation $3x + 1 = 4y$; en la comparant à l'équation générale $ax + b = cy$, on aura $a = 3$, $b = 1$, $c = 4$; et par conséquent

$$\alpha = \frac{4-1}{2} + \frac{1}{2} \sum_{u=1}^{u=4} \frac{\sin 2u\left(1 - \frac{3}{2}\right)\frac{\pi}{4}}{\sin \frac{3u\pi}{4}} = \frac{3}{2} - \frac{1}{2} \sum_{u=1}^{u=4} \frac{\sin \frac{u\pi}{4}}{\sin \frac{3u\pi}{4}} ,$$

c'est à dire

$$\alpha = \frac{3}{2} - \frac{\sin \frac{\pi}{4}}{2 \sin \frac{3\pi}{4}} - \frac{\sin \frac{2\pi}{4}}{2 \sin \frac{6\pi}{4}} - \frac{\sin \frac{3\pi}{4}}{2 \sin \frac{9\pi}{4}} = \frac{3}{2} - \frac{1}{2} + \frac{1}{2} - \frac{1}{2} = 1 \; ;$$

et toutes les valeurs de x, qui résolvent l'équation $3x + 1 = 4y$, seront données par l'équation $x = 1 + 4z$, comme on le sait d'ailleurs.

La valeur de x peut en général se calculer à l'aide des tables trigonométriques. Il est vrai que par ce moyen on n'obtiendra, le plus souvent, que des valeurs fractionnaires approchées, mais comme par supposition x ne peut avoir que des valeurs entières, on en trouvera la valeur exacte en substituant à cette valeur approchée, le nombre entier le plus voisin.

On peut observer que puisqu'on a

$$\frac{\sin\left(2b-a\right)\frac{u\pi}{c}}{\sin\frac{au\pi}{c}} = \frac{\sin\frac{2bu\pi}{c}\cos\frac{au\pi}{c} - \cos\frac{2bu\pi}{c}\sin\frac{au\pi}{c}}{\sin\frac{au\pi}{c}}$$

$$= \sin\frac{2bu\pi}{c}\cot\frac{au\pi}{c} - \cos\frac{2bu\pi}{c};$$

et que d'ailleurs

$$\sum_{u=1}^{u=c}\cos\frac{2bu\pi}{c} = -1;$$

on pourra écrire

$$x = \frac{c-1}{2} + \frac{1}{2}\sum_{u=1}^{u=c}\sin\frac{2bu\pi}{c}\cot\frac{au\pi}{c} + \frac{1}{2} = \frac{1}{2}\left(c + \sum_{u=1}^{u=c}\sin\frac{2bu\pi}{c}\cot\frac{au\pi}{c}\right);$$

et cette expression servira, aussi bien que la précédente, à résoudre la congruence proposée.

Il serait aisé d'appliquer ces principes aux congruences du premier degré à plusieurs inconnues: mais nous allons passer de préférence aux congrueuces du

second degré : et à cet effet nous rappellerons quelques propriétés élémentaires des résidus quadratiques, que nous pourrions déduire de nos formules générales, mais dont nous omettons les démonstrations à cause de leur simplicité.

1.° Si n est un nombre premier, en élevant successivement au carré tous les nombres 1, 2, 3, ... $n-1$; et divisant chaque carré par n, on aura $\frac{n-1}{2}$ restes différens (que M. Gauss a nommés résidus quadratiques de n) répétés chacun deux fois : et il restera, dans la série des nombres inférieurs à n, un nombre $\frac{n-1}{2}$ de non-résidus quadratiques.

2.° Si l'on fait $n = 2p + 1$, et que l'on représente par

$$a_1 \;,\; a_2 \;,\; a_3 \;,\; \ldots\ldots \; a_u \;,\; \ldots\ldots \; a_p \;,$$

les p résidus quadratiques de n, et par

$$b_1 \;,\; b_2 \;,\; b_3 \;,\; \ldots\ldots \; b_u \;,\; \ldots\ldots \; b_p \;,$$

les p non-résidus quadratiques, on aura les équations

$$\sum_{x=1}^{x=n} \cos \frac{2x^2\pi}{n} = 2 \sum_{u=1}^{u=p+1} \cos \frac{2a_u\pi}{n} \;;\quad \sum_{x=1}^{x=n} \sin \frac{2x^2\pi}{n} = 2 \sum_{u=1}^{u=p+1} \sin \frac{2a_u\pi}{n} \;;$$

$$\sum_{u=1}^{u=p+1} \left(\cos \frac{2a_u\pi}{n} + \cos 2\frac{b_u\pi}{n} \right) = \sum_{y=1}^{y=n} \cos \frac{2y\pi}{n} \;;\quad \sum_{u=1}^{u=p+1} \left(\sin \frac{2a_u\pi}{n} + \sin \frac{2b_u\pi}{n} \right) = \sum_{y=1}^{y=n} \sin \frac{2y\pi}{n} .$$

3.° En multipliant successivement un résidu quadratique quelconque a_r, par tous les autres, on aura la série

$$a_r\, a_1 \;,\; a_r\, a_2 \;,\; a_r\, a_3 \;,\; \ldots\ldots \; a_r\, a_p \;,$$

qui fournira de nouveau, en divisant tous ses termes par n, p restes différens, qui seront tous les résidus quadratiques de n disposés dans un ordre quelconque ;

d'où l'on déduira

$$(30)\ldots\ldots\left\{\begin{array}{l}\sum_{x=1}^{x=n}\cos\frac{2a_r x^2\pi}{n}=2\sum_{u=1}^{u=p+1}\cos\frac{2a_r a_u\pi}{n}=2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\ ;\\ \\ \sum_{x=1}^{x=n}\sin\frac{2a_r x^2\pi}{n}=2\sum_{u=1}^{u=p+1}\sin\frac{2a_r a_u\pi}{n}=2\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\ .\end{array}\right.$$

4.° En multipliant le résidu quadratique a_r, successivement par tous les non-résidus quadratiques

$$b_1\ ,\ b_2\ ,\ b_3\ ,\ \ldots\ldots\ b_u\ ,\ \ldots\ldots\ b_p\ ,$$

on aura de nouveau, après avoir divisé tous les produits par n, p restes différens, qui seront tous les non-résidus quadratiques de n, et on trouvera

$$(31)\ldots\ldots\left\{\begin{array}{l}\sum_{u=1}^{u=p+1}\cos\frac{2a_r b_u\pi}{n}=\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\ ;\\ \\ \sum_{u=1}^{u=p+1}\sin\frac{2a_r b_u\pi}{n}=\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\ .\end{array}\right.$$

5.° En multipliant le non-résidu quadratique b_r, successivement par tous les résidus quadratiques

$$a_1\ ,\ a_2\ ,\ a_3\ ,\ \ldots\ldots\ a_u\ ,\ \ldots\ldots\ a_p\ ,$$

et divisant tous les produits par n, on aura pour restes tous les non-résidus

quadratiques; et par conséquent on obtiendra

$$(32) \ldots\ldots \left\{ \begin{array}{l} \sum_{u=1}^{u=p+1} \cos \frac{2 b_r a_u \pi}{n} = \sum_{u=1}^{u=p+1} \cos \frac{2 b_u \pi}{n} ; \\ \\ \sum_{u=1}^{u=p+1} \sin \frac{2 b_r a_u \pi}{n} = \sum_{u=1}^{u=p+1} \sin \frac{2 b_u \pi}{n} . \end{array} \right.$$

6.° Enfin en multipliant successivement un non-résidu quadratique quelconque b_r, par tous les non-résidus quadratiques

$$b_1 \ , \ b_2 \ , \ b_3 \ , \ \ldots\ldots \ b_u \ , \ \ldots\ldots \ b_p \ ,$$

on aura pour restes, après avoir divisé chaque produit par n, tous les résidus quadratiques, et partant on trouvera

$$\sum_{u=1}^{u=p+1} \cos \frac{2 b_r b_u \pi}{n} = \sum_{u=1}^{u=p+1} \cos \frac{2 a_u \pi}{n} ;$$

$$\sum_{u=1}^{u=p+1} \sin \frac{2 b_r b_u \pi}{n} = \sum_{u=1}^{u=p+1} \sin \frac{2 a_u \pi}{n} .$$

Maintenant si l'on représente par N le nombre des solutions entières et moindres que n, de la congruence

$$x^2 + c \equiv 0 \pmod{n},$$

dans laquelle n est un nombre premier, on sait par ce que nous avons démontré précédemment, que N ne peut qu'être égale à zéro ou à 2, et en partant de

la formule (24), on trouvera

$$nN = \sum_{x=0}^{x=n}\left(1 + \cos 2(x^2+c)\frac{\pi}{n} + \cos 4(x^2+c)\frac{\pi}{n} \ldots\ldots + \cos 2(n-1)(x^2+c)\frac{\pi}{n}\right)$$

$$= \sum_{x=0}^{x=n}\sum_{y=0}^{y=n}\cos 2y(x^2+c)\frac{\pi}{n} = n + \sum_{y=1}^{y=n}\cos\frac{2yc\pi}{n} + \sum_{x=1}^{x=n}\sum_{y=1}^{y=n}\cos 2y(x^2+c)\frac{\pi}{n}$$

$$= n + \sum_{y=1}^{y=n}\cos\frac{2yc\pi}{n} + \sum_{x=1}^{x=n}\sum_{y=1}^{y=n}\left(\cos\frac{2yx^2\pi}{n}\cos\frac{2yc\pi}{n} - \sin\frac{2yx^2\pi}{n}\sin\frac{2yc\pi}{n}\right).$$

Si l'on substitue dans cette formule les valeurs de

$$\sum_{y=1}^{y=n}\cos\frac{2yx^2\pi}{n}\cos\frac{2yc\pi}{n} = \sum_{u=1}^{u=p+1}\left(\cos\frac{2a_u x^2\pi}{n}\cos\frac{2ca_u\pi}{n} + \cos\frac{2b_u x^2\pi}{n}\cos\frac{2cb_u\pi}{n}\right),$$

$$\sum_{y=1}^{y=n}\sin\frac{2yx^2\pi}{n}\sin\frac{2yc\pi}{n} = \sum_{u=1}^{u=p+1}\left(\sin\frac{2a_u x^2\pi}{n}\sin\frac{2ca_u\pi}{n} + \sin\frac{2b_u x^2\pi}{n}\sin\frac{2cb_u\pi}{n}\right),$$

on obtiendra

$$nN = n + \sum_{y=1}^{y=n}\cos\frac{2yc\pi}{n} + \sum_{x=1}^{x=n}\sum_{u=1}^{u=p+1}\left\{\begin{array}{l}\cos\frac{2a_u x^2\pi}{n}\cos\frac{2ca_u\pi}{n} + \cos\frac{2b_u x^2\pi}{n}\cos\frac{2cb_u\pi}{n}\\ -\sin\frac{2a_u x^2\pi}{n}\sin\frac{2ca_u\pi}{n} - \sin\frac{2b_u x^2\pi}{n}\sin\frac{2cb_u\pi}{n}\end{array}\right\};$$

ou bien, en séparant les intégrales,

$$nN = \left\{ \begin{array}{l} n + \sum\limits_{y=1}^{y=n} \cos \frac{2yc\pi}{n} + \sum\limits_{u=1}^{u=p+1} \left(\cos \frac{2ca_u\pi}{n} \sum\limits_{x=1}^{x=n} \cos \frac{2a_u x^2 \pi}{n} \right) + \sum\limits_{u=1}^{u=p+1} \left(\cos \frac{2b_u\pi}{n} \sum\limits_{x=1}^{x=n} \cos \frac{2b_u x^2 \pi}{n} \right) \\ - \sum\limits_{u=1}^{u=p+1} \left(\sin \frac{2ca_u\pi}{n} \sum\limits_{x=1}^{x=n} \sin \frac{2a_u x^2 \pi}{n} \right) - \sum\limits_{u=1}^{u=p+1} \left(\sin \frac{2cb_u\pi}{n} \sum\limits_{x=1}^{x=n} \sin \frac{2b_u x^2 \pi}{n} \right) \end{array} \right\}$$

et cette équation, à l'aide des équations (30), (31), (32), se transformera dans la suivante

$$(33) \ldots nN = \left\{ \begin{array}{l} n + \sum\limits_{y=1}^{y=n} \cos \frac{2cy\pi}{n} + 2 \sum\limits_{u=1}^{u=p+1} \left(\cos \frac{2ca_u\pi}{n} \sum\limits_{u=1}^{u=p+1} \cos \frac{2a_u\pi}{n} \right) + 2 \sum\limits_{u=1}^{u=p+1} \left(\cos \frac{2cb_u\pi}{n} \sum\limits_{u=1}^{u=p+1} \cos \frac{2b_u\pi}{n} \right) \\ -2 \sum\limits_{u=1}^{u=p+1} \left(\sin \frac{2ca_u\pi}{n} \sum\limits_{u=1}^{u=p+1} \sin \frac{2a_u\pi}{n} \right) - 2 \sum\limits_{u=1}^{u=p+1} \left(\sin \frac{2cb_u\pi}{n} \sum\limits_{u=1}^{u=p+1} \sin \frac{2b_u\pi}{n} \right) \end{array} \right\}.$$

Mais comme les quantités

$$\sum_{u=1}^{u=p+1} \cos \frac{2a_u\pi}{n}, \quad \sum_{u=1}^{u=p+1} \cos \frac{2b_u\pi}{n},$$

$$\sum_{u=1}^{u=p+1} \sin \frac{2a_u\pi}{n}, \quad \sum_{u=1}^{u=p+1} \sin \frac{2b_u\pi}{n},$$

qui sont des intégrales définies, deviennent indépendantes de u et égales à des constantes, on pourra les transporter en dehors de la première intégration dans

l'équation (33), et on aura

$$(34)\ldots\ nN=\begin{cases} n+\sum_{y=1}^{y=n}\cos\frac{2cy\pi}{n}+2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\cdot\sum_{u=1}^{u=p+1}\cos\frac{2ca_u\pi}{n}+2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\cdot\sum_{u=1}^{u=p+1}\cos\frac{2cb_u\pi}{n} \\ -2\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\cdot\sum_{u=1}^{u=p+1}\sin\frac{2ca_u\pi}{n}-2\sum_{u=1}^{u=p+1}\sin\frac{2cb_u\pi}{n}\cdot\sum_{u=1}^{u=p+1}\sin\frac{2cb_u\pi}{n}\end{cases}$$

et cette équation devra exister en même tems que les suivantes

$$(35)\ldots\ \begin{cases}\sum_{u=1}^{u=p+1}\left(\cos\frac{2a_u\pi}{n}+\cos\frac{2b_u\pi}{n}\right)=\sum_{y=1}^{y=n}\cos\frac{2y\pi}{n}=\sum_{y=1}^{y=n}\cos\frac{2cy\pi}{n}=-1\,, \\ \sum_{u=1}^{u=p+1}\left(\sin\frac{2a_u\pi}{n}+\sin\frac{2b_u\pi}{n}\right)=\sum_{y=1}^{y=n}\sin\frac{2y\pi}{n}=0\,.\end{cases}$$

A présent supposons $c=\pm 1$; $n=4m+1$; et chacune des congruences

$$x^2+1\equiv 0\ (\text{mod. } n)\ ;\quad x^2-1\equiv 0\ (\text{mod. } n)\ ;$$

aura deux solutions : par conséquent N sera égale à 2, et l'équation (34) se transformera dans la suivante

$$2n=\begin{cases} n-1+2\left(\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right)^2+2\left(\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right)^2 \\ \mp 2\left(\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\right)^2\mp 2\left(\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\right)^2\end{cases}$$

d'où l'on tirera

$$\frac{n+1}{2}=\left(\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right)^2+\left(\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right)^2;$$

$$\left(\sum_{u=1}^{u=p+1}\sin.\frac{2a_u\pi}{n}\right)^2+\left(\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\right)^2=0;$$

et puisque, par les équations (35), l'on a

$$\left(\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right)^2=\left(\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}+1\right)^2;$$

$$\left(\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\right)^2=\left(\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\right)^2;$$

on trouvera

$$n+1=4\left(\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right)^2+4\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}+2;$$

et partant

$$n=\left(2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}+1\right)^2;$$

d'où l'on déduira les équations

$$(36)\ldots\ldots\left\{\begin{array}{l} \sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}=-\frac{1}{2}\pm\frac{1}{2}\sqrt{n}\ ;\ \sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}=-\frac{1}{2}\mp\frac{1}{2}\sqrt{n}\ ; \\ \sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}=0\ ;\ \sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}=0\ . \end{array}\right.$$

Lorsque n est un nombre premier de la forme $4m+3$, si l'on fait $c=\pm 1$, la congruence $x^2-1\equiv 0 \pmod{n}$ aura deux solutions, tandis que l'autre $x^2+1\equiv 0 \pmod{n}$ ne sera pas résoluble; alors on aura les deux équations

$$2n=\left\{\begin{array}{l} n+2\left(\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right)^2+2\left(\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right)^2 \\ +2\left(\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\right)^2+2\left(\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\right)^2 \end{array}\right\};$$

$$0=\left\{\begin{array}{l} n+2\left(\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right)^2+2\left(\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right)^2 \\ -2\left(\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\right)^2-2\left(\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\right)^2 \end{array}\right\};$$

qui, étant combinées avec les équation (35), donnent

$$(37) \ldots\ldots \begin{cases} \sum_{u=1}^{u=p+1} \cos \frac{2 a_u \pi}{n} = -\frac{1}{2} \; ; \; \sum_{u=1}^{u=p+1} \cos \frac{2 b_u \pi}{n} = -\frac{1}{2} \; ; \\ \sum_{u=1}^{u=p+1} \sin \frac{2 a_u \pi}{n} = \pm \frac{1}{2} \sqrt{n} \; ; \; \sum_{u=1}^{u=p+1} \sin \frac{2 b_u \pi}{n} = \mp \frac{1}{2} \sqrt{n} \; . \end{cases}$$

Ces intégrales définies ont été données pour la première fois par M. Gauss dans ses Recherches Arithmétiques; et il les a trouvées en partant de sa théorie de la division du cercle en parties égales. Cet illustre géomètre a repris le même sujet dans un mémoire particulier où il les a démontrées de nouveau. Mais les deux démonstrations de M. Gauss, qui sont les seules connues puisqu'ici, quoique très-ingénieuses nous paraissent moins directes que celle que nous venons d'exposer, qui se déduit tout simplement de la formule fondamentale (24), avec beaucoup d'autres résultats. Cependant comme les équations (36) et (37), sont la base de tout ce que l'on sait sur les congruences du second degré, nous allons reprendre la démonstration que nous avons donnée, pour la rendre plus simple et plus claire.

On sait que lorsque $n = 2p + 1$ est un nombre premier de la forme $4m + 1$, les congruences

$$x^2 + 1 \equiv 0 \pmod{n} \quad , \quad x^2 - 1 \equiv 0 \pmod{n} \, ,$$

seront résolubles toutes deux, et auront chacune deux solutions: alors par la formule (24) on obtiendra l'équation

$$2n = \sum_{x=0}^{x=n} \begin{pmatrix} \left(\cos \frac{0\pi}{n} + \sqrt{-1} \sin \frac{0\pi}{n}\right)^{x^2 \pm 1} + \left(\cos \frac{2\pi}{n} + \sqrt{-1} \sin \frac{2\pi}{n}\right)^{x^2 \pm 1} \ldots\ldots\ldots\ldots\ldots \\ + \left(\cos \frac{2t\pi}{n} + \sqrt{-1} \sin \frac{2t\pi}{n}\right)^{x^2 \pm 1} \ldots\ldots + \left(\cos \frac{2(n-1)\pi}{n} + \sqrt{-1} \sin \frac{2(n-1)\pi}{n}\right)^{x^2 \pm 1} \end{pmatrix} ;$$

et par conséquent l'autre

$$2n = \begin{cases} \left(\cos\frac{0\pi}{n} \pm \sqrt{-1}\sin\frac{0\pi}{n}\right)\sum_{x=0}^{x=n}\left(\cos\frac{0x^2\pi}{n} + \sqrt{-1}\sin\frac{0x^2\pi}{n}\right) \\ + \left(\cos\frac{2\pi}{n} \pm \sqrt{-1}\sin\frac{2\pi}{n}\right)\sum_{x=0}^{x=n}\left(\cos\frac{2x^2\pi}{n} + \sqrt{-1}\sin\frac{2x^2\pi}{n}\right) \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ + \left(\cos\frac{2t\pi}{n} \pm \sqrt{-1}\sin\frac{2t\pi}{n}\right)\sum_{x=0}^{x=n}\left(\cos\frac{2tx^2\pi}{n} + \sqrt{-1}\sin\frac{2tx^2\pi}{n}\right) \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ + \left(\cos\frac{2(n-1)\pi}{n} \pm \sqrt{-1}\sin\frac{2(n-1)\pi}{n}\right)\sum_{x=0}^{x=n}\left(\cos\frac{2(n-1)x^2\pi}{n} + \sqrt{-1}\sin\frac{2(n-1)x^2\pi}{n}\right) \end{cases}$$

Si l'on effectue les multiplications indiquées dans cette équation, en observant que les imaginaires doivent se détruire entre eux, on trouvera

$$2n = \begin{cases} \cos\frac{0\pi}{n}\sum_{x=0}^{x=n}\cos\frac{0x^2\pi}{n} + \cos\frac{2\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2x^2\pi}{n} \dots + \cos\frac{2t\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2tx^2\pi}{n} \dots + \cos\frac{2(n-1)\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2(n-1)x^2\pi}{n} \\ \pm\left(\sin\frac{0\pi}{n}\sum_{x=0}^{x=n}\sin\frac{0x^2\pi}{n} + \sin\frac{2\pi}{n}\sum_{x=0}^{x=n}\sin\frac{2x^2\pi}{n} \dots + \sin\frac{2t\pi}{n}\sum_{x=0}^{x=n}\sin\frac{2tx^2\pi}{n} \dots + \sin\frac{2(n-1)\pi}{n}\sum_{x=0}^{x=n}\sin\frac{2(n-1)x^2\pi}{n}\right) \end{cases}$$

et partant

$$(38)\dots \begin{cases} 2n = n + \cos\frac{2\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2x^2\pi}{n} \dots + \cos\frac{2t\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2tx^2\pi}{n} \dots + \cos\frac{2(n-1)\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2(n-1)x^2\pi}{n}\,; \\ 0 = 0 + \sin\frac{2\pi}{n}\sum_{x=0}^{x=n}\sin\frac{2x^2\pi}{n} \dots + \sin\frac{2t\pi}{n}\sum_{x=0}^{x=n}\sin\frac{2tx^2\pi}{n} \dots\dots + \sin\frac{2(n-1)\pi}{n}\sum_{x=0}^{x=n}\sin\frac{2(n-1)x^2\pi}{n}\,; \end{cases}$$

Il faut observer ici que t doit prendre successivement toutes les valeurs 1, 2, 3, ... $n-1$, dout la moitié sont des résidus quadratiques dn nombre n et l'antre moitié des non-résidus quadratiques du même nombre: si l'on suppose donc t égal à un résidu quadratique quelcouque a_r, on aura

$$\cos\frac{2t\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2tx^2\pi}{n}=\cos\frac{2a_r\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2a_rx^2\pi}{n}$$

$$=\cos\frac{2a_r\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2x^2\pi}{n}=\cos\frac{2a_r\pi}{n}\left(1+2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right);$$

et l'on trouvera de même, lorsque t est un non-résidu quadratique égal à b_r,

$$\cos\frac{2b_r\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2b_rx^2\pi}{n}=\cos\frac{2b_r\pi}{n}\left(1+2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right).$$

On voit pourtant que la valeur de

$$\cos\frac{2t\pi}{n}\sum_{x=0}^{x=n}\cos\frac{2tx^2\pi}{n},$$

ne saurait être que l'une de celles-ci

$$\cos\frac{2a_r\pi}{n}\left(1+2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right);\quad\cos\frac{2b_r\pi}{n}\left(1+2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right);$$

selon que t est un résidu quadratique ou un non-résidn quadratique de n; et comme parmi les nombres 1, 2, 3, ... $n-1$, représentés par t, il y en a p qui sont résidus quadratiques de n, et autant qui ne le sont pas, on

pourra les réunir en deux groupes dans les équations (38) et on aura les équations

$$(39)\ldots\left\{\begin{aligned} n = &\left\{\begin{aligned} &\left(1 + 2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right)\left(\cos\frac{2a_1\pi}{n} + \cos\frac{2a_2\pi}{n}\ldots + \cos\frac{2a_p\pi}{n}\right)\\ &+ \left(1 + 2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right)\left(\cos\frac{2b_1\pi}{n} + \cos\frac{2b_2\pi}{n}\ldots + \cos\frac{2b_p\pi}{n}\right)\end{aligned}\right.\\ 0 = &\left\{\begin{aligned} &2\left(\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\right)\left(\sin\frac{2a_1\pi}{n} + \sin\frac{2a_2\pi}{n}\ldots\ldots + \sin\frac{2a_p\pi}{n}\right)\\ &+ 2\left(\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\right)\left(\sin\frac{2b_1\pi}{n} + \sin\frac{2b_2\pi}{n}\ldots\ldots + \sin\frac{2b_p\pi}{n}\right)\end{aligned}\right.\end{aligned}\right.$$

Mais comme l'on a

$$\cos\frac{2a_1\pi}{n} + \cos\frac{2a_2\pi}{n}\ldots\ldots + \cos\frac{2a_p\pi}{n} = \sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n};$$

$$\cos\frac{2b_1\pi}{n} + \cos\frac{2b_2\pi}{n}\ldots\ldots + \cos\frac{2b_p\pi}{n} = \sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n};$$

$$\sin\frac{2a_1\pi}{n} + \sin\frac{2a_2\pi}{n}\ldots\ldots + \sin\frac{2a_p\pi}{n} = \sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n};$$

$$\sin\frac{2b_1\pi}{n} + \sin\frac{2b_2\pi}{n}\ldots\ldots + \sin\frac{2b_p\pi}{n} = \sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n};$$

les deux équations (39) deviendront

$$n = \left(1 + 2\sum_{u=1}^{u=p+1} \cos\frac{2a_u\pi}{n}\right)\sum_{u=1}^{u=p+1} \cos\frac{2a_u\pi}{n} + \left(1 + 2\sum_{u=1}^{u=p+1} \cos\frac{2b_u\pi}{n}\right)\sum_{u=1}^{u=p+1} \cos\frac{2b_u\pi}{n} \; ;$$

$$0 = 2\left(\sum_{u=1}^{u=p+1} \sin\frac{2a_u\pi}{n}\right)^2 + 2\left(\sum_{u=1}^{u=p+1} \sin\frac{2b_u\pi}{n}\right)^2 \; ;$$

et puisque l'on a aussi

$$\sum_{u=1}^{u=p+1} \cos\frac{2a_u\pi}{n} + \sum_{u=1}^{u=p+1} \cos\frac{2b_u\pi}{n} = -1 \; ; \quad \sum_{u=1}^{u=p+1} \sin\frac{2a_u\pi}{n} + \sum_{u=1}^{u=p+1} \sin\frac{2b_u\pi}{n} = 0 \; :$$

on trouvera, en éliminant entre les quatre équations précédentes,

$$\sum_{u=1}^{u=p+1} \cos\frac{2a_u\pi}{n} = -\frac{1}{2} \pm \frac{1}{2}\sqrt{n} \; ; \quad \sum_{u=1}^{u=p+1} \cos\frac{2b_u\pi}{n} = -\frac{1}{2} \mp \frac{1}{2}\sqrt{n} \; ;$$

$$\sum_{u=1}^{u=p+1} \sin\frac{2a_u\pi}{n} = \sum_{u=1}^{u=p+1} \sin\frac{2b_u\pi}{n} = 0 \, .$$

Si n était de la forme $4m + 3$, on aurait à la place des équations (38), les

deux autres

$$n = \begin{cases} \left(1 + 2\sum_{u=1}^{u=p+1} \cos\frac{2a_u\pi}{n}\right)\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n} + \left(1 + 2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right)\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n} \\ + 2\left(\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\right)^2 + 2\left(\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\right)^2 \end{cases}$$

$$0 = \begin{cases} \left(1 + 2\sum_{u=1}^{u=p+1} \cos\frac{2a_u\pi}{n}\right)\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n} + \left(1 + 2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right)\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n} \\ - 2\left(\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\right)^2 - 2\left(\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\right)^2 \end{cases}$$

qui étant combinées avec les équations (35) donneraient

$$\sum_{u=1}^{u=p+1} \cos\frac{2a_u\pi}{n} = \sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n} = -\frac{1}{2};$$

$$\sum_{u=1}^{u=p+1} \cos\frac{2a_u\pi}{n} = \pm\frac{1}{2}\sqrt{n}\ ;\ \sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n} = \mp\frac{1}{2}\sqrt{n}\ .$$

Ces dernières équations coïncident avec celles que nous avions trouvées précédemment.

Il résulte de l'analyse précédente qu'étant proposée la congruence

$$x^2 + c \equiv 0 \pmod{n},$$

(dans laquelle n est un nombre premier égal à $2p+1$) si l'on représente par N le nombre de ses solutions, on aura

$$nN = \begin{cases} n + \left(1 + 2\sum_{u=1}^{u=p+1} \cos\frac{2a_u\pi}{n}\right)\sum_{u=1}^{u=p+1}\cos\frac{2ca_u\pi}{n} + \left(1 + 2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right)\sum_{u=1}^{u=p+1}\cos\frac{2cb_u\pi}{n} \\ -2\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}\cdot\sum_{u=1}^{u=p+1}\sin\frac{2ca_u\pi}{n} - 2\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}\cdot\sum_{u=1}^{u=p+1}\sin\frac{2cb_u\pi}{n} \end{cases}$$

Mais comme, lorsque n est de la forme $4m+1$, on a

$$\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n} = \sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n} = 0,$$

on trouvera, dans ce cas,

$$N = 1 + \frac{1}{n}\left(1 + 2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n}\right)\sum_{u=1}^{u=p+1}\cos\frac{2ca_u\pi}{n} + \frac{1}{n}\left(1 + 2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n}\right)\sum_{u=1}^{u=p+1}\cos\frac{2cb_u\pi}{n};$$

et la valeur de N restera la même quand on changera $+c$, en $-c$. Donc si la congruence

$$x^2 + c \equiv 0 \pmod{n},$$

(dans laquelle n est un nombre premier de la forme $4m+1$) est résoluble, celle-ci

$$y^2 - c \equiv 0 \pmod{n}$$

le sera de même; et si l'une d'elles n'est pas résoluble, l'autre ne le sera pas non plus.

Si $n = 2p + 1$, est un nombre premier de la forme $4m + 3$, on aura

$$1 + 2 \sum_{u=1}^{u=p+1} \cos \frac{2 a_u \pi}{n} = 1 + 2 \sum_{u=1}^{u=p+1} \cos \frac{2 b_u \pi}{n} = 0 ;$$

et le nombre N des solutions de la congruence

$$x^2 + c \equiv 0 \pmod{n},$$

sera donné par l'équation

$$(40) \ldots n N = n - 2 \sum_{u=1}^{u=p+1} \sin \frac{2 a_u \pi}{n} \sum_{u=1}^{u=p+1} \sin \frac{2 c a_u \pi}{n} - 2 \sum_{u=1}^{u=p+1} \sin \frac{2 b_u \pi}{n} \sum_{u=1}^{u=p+1} \sin \frac{2 c b_u \pi}{n} ;$$

qui se réduira, lorsque c est un résidu quadratique de n, à l'autre

$$n N = n - 2 \left(\sum_{u=1}^{u=p+1} \sin \frac{2 a_u \pi}{n} \right)^2 - 2 \left(\sum_{u=1}^{u=p+1} \sin \frac{2 b_u \pi}{n} \right)^2 = n - \frac{n}{2} - \frac{n}{2} = 0 .$$

Si l'on change $+ c$ en $- c$ dans l'équation (40), on trouvera que le nombre N des solutions de la congruence

$$y^2 - c \equiv 0 \pmod{p},$$

sera exprimé, lorsque c est un résidu quadratique de n, par l'équation

$$n N = n + 2 \left(\sum_{u=1}^{u=p+1} \sin \frac{2 a_u \pi}{n} \right)^2 + 2 \left(\sum_{u=1}^{u=p+1} \sin \frac{2 b_u \pi}{n} \right)^2 = n + \frac{n}{2} + \frac{n}{2} = 2n .$$

On déduit de là, que lorsque n est un nombre premier de la forme $4m + 3$, l'une des deux congruences

$$x^2 + c \equiv 0 \pmod{n} \quad ; \quad y^2 - c \equiv 0 \pmod{n} ;$$

sera toujours résoluble, mais qu'on ne pourra jamais les résoudre toutes deux à la fois.

En partant des équations (36) et (37) on trouve, qu'en indiquant toujours par a_r un résidu quadratique quelconque du nombre premier $n = 2p + 1$, et par b_r un non-résidu quadratique quelconque du même nombre, on aura, lorsque n est de la forme $4m + 1$,

$$\sum_{x=0}^{x=n}\left(\cos\frac{2a_r x^2\pi}{n} + \sqrt{-1}\,\sin\frac{2a_r x^2\pi}{n}\right) = 1 + 2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n} + 2\sqrt{-1}\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}$$

$$= 1 + 2\left(-\frac{1}{2} \pm \frac{1}{2}\sqrt{n}\right) = \pm\sqrt{n}\ ;$$

$$\sum_{x=0}^{x=n}\left(\cos\frac{2b_r x^2\pi}{n} + \sqrt{-1}\,\sin\frac{2b_r x^2\pi}{n}\right) = 1 + 2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n} + 2\sqrt{-1}\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}$$

$$= 1 + 2\left(-\frac{1}{2} \mp \frac{1}{2}\sqrt{n}\right) = \mp\sqrt{n}\ ;$$

tandis que lorsque n est de la forme $4m + 3$, on trouvera

$$\sum_{x=0}^{x=n}\left(\cos\frac{2a_r x^2\pi}{n} + \sqrt{-1}\,\sin\frac{2a_r x^2\pi}{n}\right) = 1 + 2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n} + 2\sqrt{-1}\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}$$

$$= 1 + 2\left(-\frac{1}{2}\right) + 2\sqrt{-1}\left(\pm\frac{1}{2}\sqrt{n}\right) = \pm\sqrt{-n}\ ;$$

$$\sum_{x=0}^{x=n}\left(\cos\frac{2b_r x^2\pi}{n} + \sqrt{-1}\,\sin\frac{2b_r x^2\pi}{n}\right) = 1 + 2\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n} + 2\sqrt{-1}\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}$$

$$= 1 + 2\left(-\frac{1}{2}\right) + 2\sqrt{-1}\left(\mp\frac{1}{2}\sqrt{n}\right) = \mp\sqrt{-n}\ ;$$

de sorte que l'on obtiendra en général les équations

$$\sum_{x=0}^{x=n}\left(\cos\frac{2a_r x^2\pi}{n}+\sqrt{-1}\sin\frac{2a_r x^2\pi}{n}\right)=\pm\sqrt{n(-1)^{\frac{n-1}{2}}}\;;$$

$$\sum_{x=0}^{x=n}\left(\cos\frac{2b_r x^2\pi}{n}+\sqrt{-1}\sin\frac{2b_r x^2\pi}{n}\right)=\mp\sqrt{n(-1)^{\frac{n-1}{2}}}\;.$$

Maintenant soit proposé de trouver le nombre N des solutions entières et moindres que n, de la congruence

$$x^2+ay^2+b\equiv 0 \quad (\text{mod. } n)\;,$$

dans laquelle n est un nombre premier, et a, b, sont des nombres entiers non divisibles par n; il est clair que par la formule (24) on obtiendra l'équation

$$nN=\sum_{x=0}^{x=n}\sum_{y=0}^{y=n}\left(1+\left(\cos\frac{2\pi}{n}+\sqrt{-1}\sin\frac{2\pi}{n}\right)^{x^2+ay^2+b}\ldots+\left(\cos 2(n-1)\frac{\pi}{n}+\sqrt{-1}\sin 2(n-1)\frac{\pi}{n}\right)^{x^2+ay^2+b}\right)=$$

$$n^2+\left(\cos\frac{2b\pi}{n}+\sqrt{-1}\sin\frac{2b\pi}{n}\right)\sum_{x=0}^{x=n}\left(\cos\frac{2x^2\pi}{n}+\sqrt{-1}\sin\frac{2x^2\pi}{n}\right)\sum_{y=0}^{y=n}\left(\cos\frac{2ay^2\pi}{n}+\sqrt{-1}\sin\frac{2ay^2\pi}{n}\right)$$

$$+\left(\cos\frac{4b\pi}{n}+\sqrt{-1}\sin\frac{4b\pi}{n}\right)\sum_{x=0}^{x=n}\left(\cos\frac{4x^2\pi}{n}+\sqrt{-1}\sin\frac{4x^2\pi}{n}\right)\sum_{y=0}^{y=n}\left(\cos\frac{4ay^2\pi}{n}+\sqrt{-1}\sin\frac{4ay^2\pi}{n}\right)$$

. . . .

$$+\left(\cos 2(n-1)\frac{b\pi}{n}+\sqrt{-1}\sin 2(n-1)\frac{b\pi}{n}\right)\sum_{x=0}^{x=n}\left(\cos 2(n-1)\frac{x^2\pi}{n}+\sqrt{-1}\sin 2(n-1)\frac{x^2\pi}{n}\right)\sum_{y=0}^{y=n}\left(\cos 2(n-1)\frac{ay^2\pi}{n}+\sqrt{-1}\sin 2(n-1)\frac{ay^2\pi}{n}\right)$$

et le valeur de N dépendra des nombres a et b.

Supposons d'abord que a et b, soient tous les deux des résidus quadratiques de n, et nous aurons, eu substituant dans l'équation précédente les valeurs déjà trouvées,

$$nN = \left\{ \begin{array}{l} n^2 + \left(-\frac{1}{2} \pm \frac{1}{2}\sqrt{n(-1)^{\frac{n-1}{2}}}\right)\left(\pm\sqrt{n(-1)^{\frac{n-1}{2}}}\right)\left(\pm\sqrt{n(-1)^{\frac{n-1}{2}}}\right) \\ + \left(-\frac{1}{2} \mp \frac{1}{2}\sqrt{n(-1)^{\frac{n-1}{2}}}\right)\left(\mp\sqrt{n(-1)^{\frac{n-1}{2}}}\right)\left(\mp\sqrt{n(-1)^{\frac{n-1}{2}}}\right) \end{array} \right\}$$

$$= n^2 - n(-1)^{\frac{n-1}{2}}.$$

Lorsque a et b, sont tous les deux non-résidus quadratiques de n on obtiendra

$$nN = n^2 + n(-1)^{\frac{n-1}{2}}.$$

Lorsque a est un résidu quadratique de n, et b un non-résidu quadratique du même nombre on aura

$$nN = n^2 - n(-1)^{\frac{n-1}{2}}.$$

Et enfin lorsque a est un non-résidu quadratique de n, et b un résidu quadratique du même nombre, on trouvera

$$nN = n^2 + n(-1)^{\frac{n-1}{2}}.$$

Il résulte de là, que la congruence

$$x^2 + ay^2 + b \equiv 0 \pmod{n},$$

dans laquelle n est un nombre premier, aura toujours un nombre $n \pm 1$ de solutions.



Lagrange a démontré pour la première fois que la congruence

$$x^2 + ay^2 + b \equiv 0 \quad (\text{mod. } n) ,$$

était toujours résoluble, lorsque le nombre premier n ne divisait ni a ni b. Cet illustre géomètre est parti de ce théorème pour démontrer qu'un nombre entier quelconque est toujours la somme de quatre carrés en nombres entiers : mais sa méthode ne saurait servir à déterminer le nombre des solutions de la congruence proposée, comme nous l'avons fait en partant de notre formule fondamentale (24). Il est clair que l'on pourrait appliquer les mêmes principes aux congruences du second degré, qui renferment un plus grand nombre d'inconnues. Mais nous allons nous occuper de préférence de la résolution des équations à deux termes.

On a vu que lorsque $n = 2p + 1$ est un nombre premier de la forme $4m + 1$, on trouve

$$\sum_{u=1}^{u=p+1}\left(\cos\frac{2t^2\pi}{n} + \sqrt{-1}\,\sin\frac{2t^2\pi}{n}\right)^{a_u} = -\frac{1}{2} \pm \frac{1}{2}\sqrt{n} ;$$

$$\sum_{u=1}^{u=p+1}\left(\cos\frac{2t^2\pi}{n} + \sqrt{-1}\,\sin\frac{2t^2\pi}{n}\right)^{b_u} = -\frac{1}{2} \mp \frac{1}{2}\sqrt{n} ;$$

en indiquant toujours par a_u un résidu quadratique quelconque de n, par b_u un non-résidu quadratique de n, et par t un nombre entier non divisible par n. Si l'on fait maintenant

$$\cos\frac{2t^2\pi}{n} + \sqrt{-1}\,\sin\frac{2t^2\pi}{n} = r^{t^2} ,$$

r exprimant la racine

$$x = \cos\frac{2\pi}{n} + \sqrt{-1}\,\sin\frac{2\pi}{n} ,$$

de l'équation

$$X = \frac{x^n - 1}{x - 1} = 0 ,$$

on aura, par ce qui précède,

$$(41)\ldots\ldots \quad X_1 = x^{a_1} + x^{a_2} \ldots\ldots\ldots + x^{a_p} + \frac{1}{2} \mp \frac{1}{2}\sqrt{n} = 0 ;$$

et cette équation, qui sera satisfaite par la valeur $x = r$, le sera aussi par toutes les autres valeurs

$$x = r^{2^2} ; \; x = r^{3^2} ; \; \ldots\ldots x = r^{(n-1)^2} ;$$

dont le nombre se réduira à la moitié puisque $r^{s^2} = r^{(n-s)^2}$. Mais comme ces racines résolvent l'équation $X = 0$, elles seront communes aux deux équations $X = 0$, $X_1 = 0$. Les autres racines qui résolvent l'équation $X = 0$, sans résoudre l'équation $X_1 = 0$, seront de la forme

$$x = r^{b_1} ; \; x = r^{b_2} ; \; \ldots\ldots x = r^{b_p} ;$$

et ne pourront pas résoudre l'équation $X_1 = 0$; car si l'une d'elles, r^{b_1} par exemple, pouvait résoudre cette équation, comme on a toujours

$$r^{b_t a_u} = r^{b_t} ,$$

en substituant cette racine supposée $x = r^{b_t}$, dans l'équation $X_1 = 0$, elle deviendrait de la forme

$$r^{b_1} + r^{b_2} \ldots\ldots + r^{b_p} + \frac{1}{2} \mp \frac{1}{2}\sqrt{n} = 0 ;$$

mais cette équation est absurde puisque l'on a

$$r^{b_1} + r^{b_2} \ldots\ldots + r^{b_p} + \frac{1}{2} \pm \frac{1}{2}\sqrt{n} = 0 .$$

Donc les deux équations $X = 0$, $X_1 = 0$, auront les p racines communes

$$r^{a_1} \;,\; r^{a_2} \;,\; \ldots\ldots r^{a_p} \;;$$

et en cherchant le plus grand commun diviseur Δ entre X et X_1, on aura l'équation $\Delta = 0$ qui sera du degré $\frac{n-1}{2}$, et qui contiendra toutes les racines de la forme $x = r^{a_1}$.

Si $n = 2p + 1$, était de la forme $4m + 3$, au lieu de l'équation (41), on aurait trouvé l'autre

$$X_2 = x^{a_1} + x^{a_2} \ldots\ldots + x^{a_p} + \frac{1}{2} \mp \frac{1}{2}\sqrt{-n} = 0 \;;$$

et en cherchant le plus grand diviseur commun entre

$$X = \frac{x^n - 1}{x - 1} = 0 \;,\; \text{et } X_2 = 0 \;,$$

on obtiendrait l'équation qui a p racines de la forme

$$x = r^{a_1} \;,\; x = r^{a_2} \;,\; \ldots\ldots x = r^{a_p} \;,$$

et l'équation $X = 0$, serait encore décomposée en deux autres du degré $\frac{n-1}{2}$.

Il faut remarquer ici que lorsque n est un nombre premier de la forme $4m + 1$, les coefficiens des diverses puissances de x dans l'équation $\Delta = 0$,

sont des fonctions de $-\frac{1}{2} \pm \frac{1}{2}\sqrt{n}$ en général; tandis que les coefficiens des puissances correspondantes dans l'équation $\frac{X}{\Delta} = \Delta_1 = 0$, sont des fonctions semblables de $-\frac{1}{2} \mp \frac{1}{2}\sqrt{n}$. En effet, si l'on fait

$$\Delta = x^p + A_1\, x^{p-1} \ldots\ldots + A_p = 0\ ;$$

$$\Delta_1 = x^p + B_1\, x^{p-1} \ldots\ldots + B_p = 0\ ;$$

les coefficiens A_1, A_2, ... A_p, pourront s'exprimer exclusivement par la somme des puissances des racines de l'équation $\Delta = 0$, somme que nous indiquerons en général par P_r ; et les coefficiens B_1, B_2, ... B_p, s'exprimeront de la même manière par la somme des puissances des racines de l'équation $\Delta_1 = 0$, somme que nous indiquerons en général par P_r ; et comme lorsque r n'est pas un multiple de n on a toujours

$$P_r = -\frac{1}{2} \pm \frac{1}{2}\sqrt{n}\ ;\quad P_r + \mathrm{P}_r = -1\ ;\quad \mathrm{P}_r = -\frac{1}{2} \mp \frac{1}{2}\sqrt{n}\ ;$$

il n'y aura d'autre différence entre P_r et P_r, que dans le signe de $\frac{1}{2}\sqrt{n}$; par conséquent si l'on désigne par Y la somme de tous les termes de l'équation $\Delta = 0$, qui ne contiennent pas $\sqrt{n}$; et par $Z\sqrt{n}$, la somme de tous ceux qui contiennent $\sqrt{n}$, on aura

$$\Delta = Y + Z\sqrt{n}\ ;\quad \Delta_1 = Y - Z\sqrt{n}\ ;$$

et partant

$$X = \frac{x^n - 1}{x - 1} = \Delta\,\Delta_1 = Y^2 - n\,Z^2 \,.$$

Si n était de la forme $4\,m + 3$, on trouverait

$$X = Y^2 + n\,Z^2 \;;$$

et en général on obtiendra

$$X = Y^2 - n\,Z^2\,(-1)^{\frac{n-1}{2}} \,,$$

n étant un nombre premier quelconque, et Y, Z, étant des fonctions entières et rationnelles de x. On trouvera aisément, par la comparaison des coefficiens dans l'équation

$$\Delta\,\Delta_1 = \frac{x^n - 1}{x - 1} \,,$$

que les coefficiens numériques des diverses puissances de x dans les équations $\Delta = 0$, $\Delta_1 = 0$, ne peuvent admettre d'autre diviseur que le nombre 2; et l'on déduira de là que l'équation

$$\frac{4\,(x^n - 1)}{x - 1} = Y^2 \pm n\,Z^2$$

(dans laquelle Y et Z, sont deux polynomes en x entiers et rationnels, à coefficiens entiers) aura toujours lieu.

Pour donner une application de ce théorème à la théorie des congruences, nous observerons que puisque la congruence

$$x^a - 1 \equiv 0 \pmod{n} \,,$$

a toujours a solutions lorsque n est un nombre premier de la forme $a\,r + 1$;

et puisque, si a est un nombre premier impair on a aussi

$$4\,(x^a - 1) = (x - 1)\,(Y^2 \pm a\,Z^2)\,,$$

il s'ensuit que $\mp a$ est résidu quadratique de $a\,r + 1$, où il faut prendre le signe $\pm$ si a est de la forme $4\,m + 1$, et le signe $-$ si a est de la forme $4\,m + 3$. On déduit aussi de ce qui précède que lorsque a est un nombre premier on peut toujours résoudre l'équation

$$(4\,a)^n = x^2 \pm a y^2$$

en nombres entiers, quel que soit l'exposant n, pourvu qu'il reste toujours entier et positif, dans laquelle il faut prendre le signe $+$ si a est de la forme $4\,m + 3$, et le signe $-$ lorsque a est de la forme $4\,m + 1$. On trouve de même que l'équation

$$5^a = x^2 \mp a\,y^2 + 1\,,$$

est toujours résoluble en nombres entiers, lorsque a est un nombre premier quelconque: et il serait facile de trouver un grand nombre de propositions de la même nature.

Dans l'équation

$$A = \sum_{x=0}^{x=n} \left(\cos \frac{2\,x^2\,\pi}{n} + \sqrt{-1}\,\sin \frac{2\,x^2\,\pi}{n} \right) = \pm \sqrt{n\,(-1)^{\frac{n-1}{2}}}\,,$$

trouvée précédemment, on n'a pas déterminé le signe du radical: cependant en observant que l'on a

$$A = (2\sqrt{-1})^{\frac{n-1}{2}} \sin \frac{2\pi}{n} \sin \frac{6\pi}{n} \sin \frac{10\pi}{n} \ldots\ldots \sin 2\,(n-2)\,\frac{\pi}{n}\,,$$

et en cherchant combien de sinus positifs et de sinus négatifs il y aura dans le second membre de cette équation, on trouvera que, quelle que soit la forme du

nombre premier n, il faut toujours prendre le radical avec le signe $+$ dans la valeur de A. Maintenant en faisant $n = 2p + 1$, et en exprimant toujours par a_u un résidu quadratique quelconque du nombre premier n, et par b_u un non-résidu quadratique du même nombre, on aura les deux équations

$$(42)\ldots\left\{\begin{aligned}&\sum_{u=1}^{u=p+1}\left(\cos\frac{2a_u\pi}{n}+\sqrt{-1}\,\sin\frac{2a_u\pi}{n}\right)=-\frac{1}{2}+\frac{1}{2}\sqrt{\pm n}\ ;\\&\sum_{u=1}^{u=p+1}\left(\cos\frac{2b_u\pi}{n}+\sqrt{-1}\,\sin\frac{2b_u\pi}{n}\right)=-\frac{1}{2}-\frac{1}{2}\sqrt{\pm n}\ ;\end{aligned}\right.$$

dans les seconds membres desquelles il faut prendre le signe $+$, lorsque $n = 4m + 1$, et le signe $-$, lorsque $n = 4m + 3$.

Dans l'équation

$$\frac{4(x^n - 1)}{x - 1} = Y^2 \pm n Z^2\ ;$$

il y a plusieurs manières de trouver les coefficiens de x dans les polynomes Y et Z; et ces manières sont tout à fait indépendantes, comme l'on sait, de la considération des résidus quadratiques. Maintenant, parmi les deux équations

$$Y + Z\sqrt{\pm n} = 0\ ;\quad Y - Z\sqrt{\pm n} = 0\ ;$$

que nous avons déjà trouvées, il y en a toujours une qui a toutes ses racines de la forme

$$x = \cos\frac{2a_r\pi}{n} + \sqrt{-1}\,\sin\frac{2a_r\pi}{n}\ ,$$

en prenant pour a_r successivement tous les résidus quadratiques de n ; tandis

que l'autre de ces deux équations aura ses racines de la forme

$$x = \cos \frac{2 b_r \pi}{n} + \sqrt{-1} \sin \frac{2 b_r \pi}{n} \quad ,$$

en prenant successivement pour b_r, tous les non-résidus quadratiques de n. Il résulte de là une méthode directe pour savoir si un nombre quelconque est résidu quadratique, ou non-résidu quadratique d'un nombre premier donné.

En effet si l'on ordonne l'équation

$$\frac{1}{2} Y + \frac{1}{2} Z \sqrt{n} = 0 \quad ,$$

par les puissances descendantes de x, on pourra, par les formules connues, trouver la somme des puissances de ses racines; alors en appellant P_a la somme des puissances a.^{mes} des racines de cette équation, on aura en général $P_a = P_1$, si a est un résidu quadratique de n, et $P_a = 1 - P_1$ dans le cas contraire.

On doit remarquer ici que comme les coefficiens de x, dans les polynomes Y et Z, se déterminent d'après la forme de n, et non d'après sa valeur numérique, on pourra transporter à tous les nombres premiers d'une forme donnée, les théorèmes qu'on aura trouvés par induction pour des petits nombres. Cette proposition, qui est de la plus haute importance, mériterait de longs développemens que nous réservons pour un travail particulier. On en peut déduire des conséquences fort singulières sur la manière de vérifier *les résultats de l'observation dans l'analyse pure*, en suivant la route tracée par Euler dans cette branche de l'algèbre, route qui a été quittée trop tôt par les géomètres. On pourrait tirer aussi de là, la démonstration de la loi de réciprocité énoncée d'abord par M. Legendre; mais comme M. Gauss a déjà donné cette démonstration en partant des équations (42), nous ne nous arrèterons pas plus long temps sur ce sujet, puisque ce qui précède renferme toute la théorie des congruences du second degré, déduite de la seule équation fondamentale (24). Mais en partant de cette même équation nous allons reprendre la résolution générale des équations à deux termes: en commençant par énoncer quelques propositions sur les résidus de tous les degrés, dont nous omettons les démonstrations qui sont très-faciles à retrouver.

1.° Supposons que $n = ap + 1$, soit un nombre premier quelconque, et que l'on élève successivement à la puissance a tous les nombres

$$1 \;,\; 2 \;,\; 3 \;,\; \ldots\ldots\; ap \;;$$

si l'on divise toutes ces puissances par n, on obtiendra p résidus du degré a, différens entre eux et plus petits que n, qui seront chacun répétés a fois. En appellant

$$\mathrm{a}_1 \;,\; \mathrm{a}_2 \;,\; \mathrm{a}_3 \;,\; \ldots\ldots\; \mathrm{a}_r \;,\; \ldots\ldots\; \mathrm{a}_p \;;$$

les résidus trouvés de cette manière, et en multipliant l'un quelconque a_r de ces résidus par la suite des puissances

$$1^a \;,\; 2^a \;,\; 3^a \;,\; \ldots\ldots\; (pa)^a \;;$$

on obtiendra de nouveau, après avoir divisé par n, la série des nombres

$$\mathrm{a}_1 \;,\; \mathrm{a}_2 \;,\; \mathrm{a}_3 \;,\; \ldots\ldots\; \mathrm{a}_r \;,\; \ldots\ldots\; \mathrm{a}_p \;;$$

disposés dans un ordre quelconque et répétés chacun a fois; et par conséquent l'on aura

$$\sum_{x=0}^{x=n} \cos \frac{2\,\mathrm{a}_r x^a \pi}{n} = \sum_{x=0}^{x=n} \cos \frac{2\,x^a \pi}{n} = 1 + a \sum_{u=1}^{u=p+1} \cos \frac{2\,\mathrm{a}_u \pi}{n} \;;$$

$$\sum_{x=0}^{x=n} \sin \frac{2\,\mathrm{a}_r x^a \pi}{n} = \sum_{x=0}^{x=n} \sin \frac{2\,x^a \pi}{n} = a \sum_{u=1}^{u=p+1} \sin \frac{2\,\mathrm{a}_u \pi}{n} \,.$$

2.° Si à présent l'on ôte les p nombres

$$\mathrm{a}_1 \;,\; \mathrm{a}_2 \;,\; \mathrm{a}_3 \;,\; \ldots\ldots\; \mathrm{a}_r \;,\; \ldots\ldots\; \mathrm{a}_p \;,$$

de la série des nombres

$$1 \;,\; 2 \;,\; 3 \;,\; \ldots\ldots \; ap \;;$$

et que l'on prenne un nombre quelconque b_r parmi les $(a-1)p$ nombres qui restent, on aura, en multipliant b_r successivement par toutes les puissances

$$1^a \;,\; 2^a \;,\; 3^a \;,\; \ldots\ldots\ldots \; (pa)^a \;,$$

et divisant chaque produit par n, un nombre p de restes divers entre eux et plus petits que n, répétés chacun a fois et qui seront tous différens des nombres

$$a_1 \;,\; a_2 \;,\; a_3 \;,\; \ldots\ldots \; a_r \;,\; \ldots\ldots \; a_p \;.$$

Si l'on appelle

$$b_1 \;,\; b_2 \;,\; b_3 \;,\; \ldots\ldots \; b_r \;,\; \ldots\ldots \; b_p \;,$$

ces nouveaux restes, en multipliant l'un quelconque d'entre eux b_r, successivement par toutes les puissances

$$1^a \;,\; 2^a \;,\; 3^a \;,\; \ldots\ldots\ldots \; (pa)^a \;,$$

on aura de nouveau les nombres

$$b_1 \;,\; b_2 \;,\; b_3 \;,\; \ldots\ldots \; b_r \;,\; \ldots\ldots \; b_p \;,$$

disposés dans un ordre quelconque et répétés chacun a fois: de manière que l'on obtiendra

$$\sum_{x=0}^{x=n} \cos \frac{2 b_r x^a \pi}{n} = 1 + a \sum_{u=1}^{u=p+1} \cos \frac{2 b_u \pi}{n} \;;$$

$$\sum_{x=0}^{x=n} \sin \frac{2 b_r x^a \pi}{n} = a \sum_{u=1}^{u=p+1} \sin \frac{2 b_u \pi}{n} \;.$$

3.° On pourrait de même obtenir les séries

$$\begin{array}{lllllll} c_1 , & c_2 , & c_3 , & \ldots\ldots & c_r , & \ldots\ldots & c_p ; \\ d_1 , & d_2 , & d_3 , & \ldots\ldots & d_r , & \ldots\ldots & d_p ; \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots ; \\ r_1 , & r_2 , & r_3 , & \ldots\ldots & r_r , & \ldots\ldots & r_p ; \end{array}$$

toutes composées de p termes différens, et qui jouissent de propriétés analogues aux séries

$$\begin{array}{lllllll} a_1 , & a_2 , & a_3 , & \ldots\ldots & a_r , & \ldots\ldots & a_p ; \\ b_1 , & b_2 , & b_3 , & \ldots\ldots & b_r , & \ldots\ldots & b_p ; \end{array}$$

et le nombre de toutes ces séries serait égal à a ; de manière qu'en réunissant les nombres qui les composent, on aurait de nouveau tous les nombres

$$1 , 2 , 3 , \ldots\ldots\ldots ap .$$

4.° Il serait aisé de démontrer que parmi les a séries que nous avons trouvées, il en existe un nombre b (qui est égal au nombre des nombres entiers plus petits que a , et qui n'ont pas de commun diviseur avec a) de la forme

$$\begin{array}{lllllll} e_1 , & e_2 , & e_3 , & \ldots\ldots & e_r , & \ldots\ldots & e_p ; \\ f_1 , & f_2 , & f_3 , & \ldots\ldots & f_r , & \ldots\ldots & f_p ; \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \text{etc.} ; \end{array}$$

qui jouissent de cette propriété, qu'en multipliant un terme quelconque e_r d'une de ces séries, par tous les autres termes de la même suite, on aura l'une des a séries que nous avons trouvées précédemment ; puis en multipliant par e^2_r , la même série, on aura une autre de ces séries, et ainsi de suite jusqu'à e^a_r ; mais cette proposition est tout à fait étrangère aux recherches suivantes.



Maintenant, si l'on fait, pour abréger,

$$1 + a \sum_{u=1}^{u=p+1} \left(\cos \frac{2\,\mathrm{a}_u\,\pi}{n} + \sqrt{-1} \sin \frac{2\,\mathrm{a}_u\,\pi}{n} \right) = 1 + a\,\mathrm{A}\ ;$$

$$1 + a \sum_{u=1}^{u=p+1} \left(\cos \frac{2\,\mathrm{b}_u\,\pi}{n} + \sqrt{-1} \sin \frac{2\,\mathrm{b}_u\,\pi}{n} \right) = 1 + a\,\mathrm{B}\ ;$$

. . . .

$$1 + a \sum_{u=1}^{u=p+1} \left(\cos \frac{2\,\mathrm{r}_u\,\pi}{n} + \sqrt{-1} \sin \frac{2\,\mathrm{r}_u\,\pi}{n} \right) = 1 + a\,\mathrm{R}\ ;$$

et que l'on considère la congruence

$$x^a + 1 \equiv 0 \quad (\text{mod. } n)\ ,$$

on sait que le nombre N_1 de ses solutions entières, positives et moindres que n, est exprimé par l'équation

$$n\,\mathrm{N}_1 = \sum_{y=0}^{y=n} \sum_{x=0}^{x=n} \left(\cos 2y\,(x^a + 1)\,\frac{\pi}{n} + \sqrt{-1} \sin 2y\,(x^a + 1)\,\frac{\pi}{n} \right)\ ;$$

qui se réduira à l'autre

$$n\,\mathrm{N}_1 = n + \mathrm{A}\,(1 + a\,\mathrm{A}) + \mathrm{B}\,(1 + a\,\mathrm{B}) \ldots\ldots + \mathrm{R}\,(1 + a\,\mathrm{R})\ ;$$

en distribuant les nombres $1, 2, 3, \ldots\ldots ap$, en groupes, comme nous l'avons indiqué précédemment.

Si l'on cherche à présent le nombre N_2 des solutions entières, positives et

moindres que n, de la congruence à deux inconnues

$$x^a + u^a + 1 \equiv 0 \quad (\text{mod. } n),$$

on aura l'équation

$$n\,N_2 = \sum_{y=0}^{y=n} \sum_{x=0}^{x=n} \sum_{u=0}^{u=n} \left(\cos 2y(x^a + u^a + 1)\frac{\pi}{n} + \sqrt{-1}\, \sin 2y(x^a + u^a + 1)\frac{\pi}{n} \right),$$

qui se réduira à l'autre

$$n\,N_2 = n^2 + A(1 + a\,A)^2 + B(1 + a\,B)^2 \ldots\ldots\ldots + R(1 + a\,R)^2 .$$

De même en cherchant le nombre N_3 des solutions entières, positives et moindres que n, de la congruence à trois inconnues

$$x^a + u^a + v^a + 1 \equiv 0 \quad (\text{mod. } n),$$

on aura une équation de la forme

$$n\,N_3 = n^3 + A(1 + a\,A)^3 + B(1 + a\,B)^3 \ldots\ldots + R(1 + a\,R)^3 ;$$

et ainsi de suite jusqu'à la congruence (qui renferme $a - 1$ inconnues)

$$x^a + u^a + v^a + z^a \ldots\ldots + 1 \equiv 0 \quad (\text{mod. } n),$$

dont le nombre N_{a-1} des solutions comprises entre zéro et n, fournira l'équation

$$n\,N_{a-1} = n^{a-1} + A(1 + a\,A)^{a-1} + B(1 + a\,B)^{a-1} \ldots + R(1 + a\,R)^{a-1} .$$

De cette manière on obtiendra un nombre $a - 1$ d'équatious, qui étant combinées avec l'équation connue

$$1 + A + B \ldots\ldots\ldots + R = 0 ,$$

serviront à déterminer, par l'élimination, les valeurs des a inconnues

$$A \;,\; B \;,\; \ldots\ldots \; R \;,$$

en fonction des nombres

$$n \ , \ a \ , \ N_1 \ , \ N_2 \ , \ \ldots\ldots \ N_{a-1} \ .$$

Au lieu d'effectuer cette élimination, il sera plus commode de chercher une équation

$$(43)\ldots \ Z = z^a + q_1 \, z^{a-1} + q_2 \, z^{a-2} \ \ldots\ldots \ + q_a = 0 \ ;$$

dont les a racines soient les quantités

$$A \ , \ B \ , \ \ldots\ldots \ R \ ;$$

et les coefficiens de cette équation se détermineront avec la plus grande facilité; puisqu'on déduit des équations que nous avons trouvées

$$A + B \ \ldots\ldots + R = -1 \ ;$$

$$A^2 + B^2 \ \ldots\ldots + R^2 = \frac{n N_1 - n + 1}{a} \ ;$$

$$A^3 + B^3 \ \ldots\ldots + R^3 = \frac{n N_2 - 2n N_1 - (n-1)^2}{a^2} \ ;$$

et ainsi de suite pour les autres sommes des diverses puissances des racines de l'équation (43). Maintenant les quantités

$$A \ , \ B \ , \ \ldots\ldots \ R \ ,$$

sont les diverses racines de l'équation (43); et si l'on suppose que l'on a résolu complètement cette équation, on aura une racine $z = A$; et partant en faisant

$$r = \cos\frac{2\pi}{n} + \sqrt{-1}\,\sin\frac{2\pi}{n} \ ,$$

on obtiendra

$$r^{\alpha_1} + r^{\alpha_2} \ \ldots\ldots + r^{\alpha_p} = A \ ,$$

et l'équation

$$X_1 = x^{a_1} + x^{a_2} \;\ldots\ldots + x^{a_p} - A = o\,,$$

aura p racines communes avec l'autre

$$X = \frac{x^n - 1}{x - 1}\,.$$

Donc en cherchant le plus grand commun diviseur entre X et X_1, on trouvera une équation du degré p qui aura pour racines les quantités

$$r^{a_1}\;,\; r^{a_2} \;\ldots\ldots\; r^{a_p}\;;$$

et qui sera de la forme

$$X_2 = x^p + s\,x^{p-1} + t\,x^{p-2} \;\ldots\ldots + l = o\,.$$

Pour trouver les autres facteurs de $X = o$, l'on prendra la racine $z = i$, de l'équation (43) et on faira

$$r^{b_1} + r^{b_2} \;\ldots\ldots + r^{b_p} = B\;;$$

puis l'on cherchera une transformée de l'équation $X = o$, telle que ses racines soient la somme de $p - 1$ racines de $X = o$, prises négativement et augmentées de la quantité B ; alors en appellant $X_3 = o$, cette transformée, il est clair qu'elle aura p racines communes avec l'équation $X = o$; et en cherchant le plus grand commun diviseur entre $X_3 = o$, et $X = o$, on aura une équation du degré p, qui aura pour racines

$$x = r^{b_1}\;;\; x = r^{b_2}\;;\;\ldots\ldots\; x = r^{b_p}\,.$$

On voit comment l'on pourra trouver, par un procédé analogue à celui dont nous venons de faire usage, les autres facteurs de l'équation $X = o$. On obtiendra de cette manière a équations du degré p qui étant multipliées entre elles, donneront de nouveau l'équation $X = o$. On peut encore observer qu'ayant trouvé l'équation $X_2 = o$, les autres facteurs du degré p, de l'équation $X = o$, se formeront en changeant A, en B, dans tous les cofficiens de



$X_2 = 0$; et ainsi de suite. Partant, étant donnée l'équation

$$X = \frac{x^n - 1}{x - 1} = 0 \quad ,$$

dans laquelle $n = ap + 1$, est un nombre premier quelconque, on pourra toujours la décomposer en a équations du degré p, au moyen d'une équation du degré a.

Lorsque a et p, sont deux nombres premiers, l'analyse précédente suffit pour trouver tous les facteurs de l'équation $x^n - 1 = 0$; mais si a est un nombre premier, et p est un nombre composé, en supposant $p = bcd \ldots t$ (les nombres b, c, d, ... t, étant tous les facteurs premiers de p, égaux ou inégaux entre eux) on trouvera d'abord les équations

$$1 + \mathrm{A} + \mathrm{B} \ldots\ldots + \mathrm{R} = 0 \; ;$$

$$n\mathrm{N}_1 = n + \mathrm{A}(1 + a\mathrm{A}) + \mathrm{B}(1 + a\mathrm{B}) \ldots + \mathrm{R}(1 + a\mathrm{R}) \; ;$$

$$n\mathrm{N}_2 = n^2 + \mathrm{A}(1 + a\mathrm{A})^2 + \mathrm{B}(1 + a\mathrm{B})^2 \ldots + \mathrm{R}(1 + a\mathrm{R})^2 \; ;$$

. . . .

$$n\mathrm{N}_{a-1} = n^{a-1} + \mathrm{A}(1 + a\mathrm{A})^{a-1} + \mathrm{B}(1 + a\mathrm{B})^{a-1} \ldots + \mathrm{R}(1 + a\mathrm{R})^{a-1} \; ;$$

d'où l'on déduira, comme auparavant, l'autre équation

$$Z = z^a + q_1 z^{a-1} + q_2 z^{a-2} \ldots\ldots + q_a = 0 \; ;$$

qui fournira les valeurs de

$$\mathrm{A} \; , \; \mathrm{B} \; , \ldots\ldots \; \mathrm{R} \; ;$$

puis l'on cherchera les valeurs de

$$N_1 \; , \; N_2 \; , \; N_3 \; , \ldots \; N_q \; , \ldots \; N_{ab-1} \; ,$$

en exprimant en général par N_q le nombre des solutions entières, positives et

moindres que n, de la congruence à q inconnues de la forme

$$x^{ab} + z^{ab} + v^{ab} \ldots\ldots + 1 \equiv 0 \pmod{n} ;$$

et l'on aura les équations

$$n\,N_1 = n + \sum_{y=1}^{y=n}\sum_{x=0}^{x=n}\left(\cos 2y(x^{ab}+1)\frac{\pi}{n} + \sqrt{-1}\,\sin 2y(x^{ab}+1)\frac{\pi}{n}\right) ;$$

$$n\,N_2 = n^2 + \sum_{y=1}^{y=n}\sum_{x=0}^{x=n}\sum_{z=0}^{z=n}\left(\cos 2y(x^{ab}+z^{ab}+1)\frac{\pi}{n} + \sqrt{-1}\,\sin 2y(x^{ab}+z^{ab}+1)\frac{\pi}{n}\right) ;$$

. . . .

$$n\,N_{ab-1} = n^{ab-1} + \sum_{y=1}^{y=n}\sum_{x=0}^{x=n}\sum_{z=0}^{z=n}\sum_{v=0}^{v=n}\ldots\left(\cos 2y(x^{ab}+z^{ab}+v^{ab}\ldots+1)\frac{\pi}{n} + \sqrt{-1}\,\sin 2y(x^{ab}+z^{ab}+v^{ab}\ldots+1)\frac{\pi}{n}\right) .$$

En décomposant en plusieurs séries les nombres

$$1\ ,\ 2\ ,\ 3\ ,\ \ldots\ldots\ n-1\ ,$$

et en classant les résidus et les non-résidus de l'ordre ab, par rapport au nombre n, comme nous l'avons déjà fait relativement aux résidus et aux non-résidus de l'ordre a, on pourra donner aux équations précédentes la forme suivante

$$\left(\begin{array}{l} 1 + A_1 + A_2 \ldots\ldots\ldots + A_b \\ \quad + B_1 + B_2 \ldots\ldots\ldots + B_b \\ \quad\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \quad\ R_1 + R_2 \ldots\ldots\ldots + R_b \end{array}\right) = 0 ;$$

$$n\,N_1 = \left\{ \begin{array}{l} n + A_1(1 + ab\,A_1) + A_2(1 + ab\,A_2) \ldots\ldots + A_b(1 + ab\,A_b) \\ + B_1(1 + ab\,B_1) + B_2(1 + ab\,B_2) \ldots\ldots + B_b(1 + ab\,B_b) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ + R_1(1 + ab\,R_1) + R_2(1 + ab\,R_2) \ldots\ldots + R_b(1 + ab\,R_b) \end{array} \right\} ;$$

$$n\,N_2 = \left\{ \begin{array}{l} n^2 + A_1(1 + ab\,A_1)^2 + A_2(1 + ab\,A_2)^2 \ldots + A_b(1 + ab\,A_b)^2 \\ + B_1(1 + ab\,B_1)^2 + B_2(1 + ab\,B_2)^2 \ldots + B_b(1 + ab\,B_b)^2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ + R_1(1 + ab\,R_1)^2 + R_2(1 + ab\,R_2)^2 \ldots + R_b(1 + ab\,R_b)^2 \end{array} \right\} ;$$

. . . .

$$n\,N_{ab-1} = \left\{ \begin{array}{l} n^{ab-1} + A_1(1 + ab\,A_1)^{ab-1} + A_2(1 + ab\,A_2)^{ab-1} \ldots + A_b(1 + ab\,A_b)^{ab-1} \\ + B_1(1 + ab\,B_1)^{ab-1} + B_2(1 + ab\,B_2)^{ab-1} \ldots + B_b(1 + ab\,B_b)^{ab-1} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ + R_1(1 + ab\,R_1)^{ab-1} + R_2(1 + ab\,R_2)^{ab-1} \ldots + R_b(1 + ab\,R_b)^{ab-1} \end{array} \right\} .$$

Il est clair qu'à l'aide de ces équations l'on pourrait former l'équation

$$Z_1 = z^{ab} + s_1\,z^{ab-1} + s_2\,z^{ab-2} \ldots\ldots + s_{ab} = 0\ ,$$

de la même manière que nous avons déjà formé l'équation $Z = 0$. Cette équation $Z_1 = 0$, aura pour racines toutes les quantités

$$\begin{array}{llllll} A_1\ , & A_2\ , & A_3\ , & \ldots\ldots & A_b\ ; \\ B_1\ , & B_2\ , & B_3\ , & \ldots\ldots & B_b\ ; \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ R_1\ , & R_2\ , & R_3\ , & \ldots\ldots & R_b\ ; \end{array}$$

et il faut observer que l'on aura

$$A_1 + A_2 + A_3 \ldots\ldots + A_b = \mathrm{A} \;;$$
$$B_1 + B_2 + B_3 \ldots\ldots + B_b = \mathrm{B} \;;$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$R_1 + R_2 + R_3 \ldots\ldots + R_b = \mathrm{R} \;;$$

les quantités A , B , . . . R ; étant les racines de l'équation $Z = 0$.

Maintenant si l'on cherche une transformée de l'équation $Z_1 = 0$, telle qu'elle ait pour racines la somme de $b - 1$ racines de l'équation $Z_1 = 0$, prises négativement et augmentées de la quantité A ; et si l'on appelle $Z_2 = 0$, cette transformée, il est clair qu'en cherchant le plus grand commun diviseur entre $Z_1 = 0$, et $Z_2 = 0$, on aura une équation de la forme

$$Z_3 = z^b + t_1\, z^{b-1} + t_2\, z^{b-2} \ldots\ldots + t_b = 0 \;;$$

qui aura pour racines les quantités

$$A_1 \;,\; A_2 \;,\; \ldots\ldots\; A_b \;.$$

Si l'on fait à présent $u = \frac{n-1}{ab}$, et que l'on exprime par

$$a_1 \;,\; a_2 \;,\; a_3 \;,\; \ldots\ldots\; a_u \;,$$

les u restes différens que l'on obtient en divisant par n successivement toutes les puissances

$$1^{ab} \;,\; 2^{ab} \;,\; 3^{ab} \;,\; \ldots\ldots\; (n-1)^{ab} \;;$$

il est clair qu'en faisant toujours

$$r = \cos\frac{2\pi}{n} + \sqrt{-1}\,\sin\frac{2\pi}{n} \;;$$

on obtiendra

$$r^{a_1} + r^{a_2} \ldots\ldots + r^{a_u} = A_1 \;.$$

D'où il résulte que l'équation

$$x^{a_1} + x^{a_2} \ldots\ldots + x^{a_u} - A_1 = 0,$$

aura u racines communes avec l'équation $X = \frac{x^n - 1}{x - 1} = 0$. Mais comme on peut former d'autres équations semblables en prenant une autre série au lieu de la série a_1, a_2, ... a_u, en écrivant l'une des quantités A_2, A_3, ... A_b, au lieu de A_1 et en cherchant une transformée de l'équation $X = 0$, comme nous l'avons fait précédemment, on aura enfin b équations semblables, qui serviront à décomposer en facteurs l'équation $X = 0$. Nous n'avons considéré que les deux facteurs a, b, du nombre $n - 1$; mais on voit que pour les autres facteurs, il n'y aurait qu'à répéter les mêmes opérations ; de manière qu'étant donnée l'équation

$$x^n - 1 = 0,$$

dans laquelle $n = a^m b^r c^s \ldots\ldots$, on la résoudra complètement à l'aide de m équations du degré a, de r équations du degré b, et ainsi de suite.

L'analyse précédente suffit pour montrer l'esprit de notre méthode ; on voit qu'elle est très-générale, et que pour être appliquée aux cas particuliers, elle n'exige pas la connaissance des racines primitives. D'ailleurs il est clair que pour résoudre l'équation $x^n - 1 = 0$, il n'est pas nécessaire de décomposer la série des nombres 1, 2, 3, ... $n - 1$, en plusieurs séries comme nous l'avons fait, afin que l'on pût bien saisir le principe notre théorie. En effet pour décomposer l'équation $x^n - 1 = 0$, dans ses facteurs, il suffit de déterminer en nombres les valeurs de

$$\mathrm{N}_1, \quad \mathrm{N}_2, \quad \ldots\ldots \quad \mathrm{N}_{a-1};$$

$$N_1, \quad N_2, \quad \ldots\ldots \quad N_{ab-1};$$

$$\ldots\ldots\ldots\ldots\ldots\ldots \text{ etc. };$$

ce que l'on pourra toujours faire *à posteriori* pour toute valeur numérique de n.

Lorsqu'il s'agit de résoudre les congruences des degrés supérieurs au second,

on rencontre beaucoup de difficulté; et l'on ne connait aucun théorème sur les résidus cubiques, ou bicarrés. Nous allons montrer maintenant les premiers élémens de cette théorie, que nous traiterons avec plus de detail dans une autre occasion.

On sait que la congruence

$$x^3 + 1 \equiv 0 \quad (\text{mod. } n) \quad ,$$

dans laquelle n est un nombre premier de la forme $6p+1$, a toujours trois solutions entières, positives et moindres que n, et partant on a par la formule (24)

$$3n = \sum_{x=0}^{x=n} \left\{ \begin{array}{l} 1 + \left(\cos 2(x^3+1)\frac{\pi}{n} + \sqrt{-1}\,\sin 2(x^3+1)\frac{\pi}{n}\right) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ + \left(\cos 2(n-1)(x^3+1)\frac{\pi}{n} + \sqrt{-1}\,\sin 2(n-1)(x^3+1)\frac{\pi}{n}\right) \end{array} \right\}.$$

Maintenant si l'on décompose la série des nombres

$$1 \;,\; 2 \;,\; 3 \;,\; \ldots\ldots \; n-1 \;,$$

dans les trois séries

$$\begin{array}{l} a_1 \;,\; a_2 \;,\; a_3 \;,\; \ldots\ldots \; a_{2p} \;, \\ b_1 \;,\; b_2 \;,\; b_3 \;,\; \ldots\ldots \; b_{2p} \;, \\ c_1 \;,\; c_2 \;,\; c_3 \;,\; \ldots\ldots \; c_{2p} \;, \end{array}$$

dont la première est la série des résidus cubiques de n, tandis que la seconde se forme en prenant un nombre quelconque de la série

$$1 \;,\; 2 \;,\; 3 \;,\; \ldots\ldots \; n-1 \;,$$

qui ne soit pas compris dans la série des résidus cubiques de n, et après avoir multiplié ce nombre successivement par tous les résidus cubiques de n, en divisant chaque produit par n; car les restes de ces divisions fourniront la série

$$b_1 \;,\; b_2 \;,\; b_3 \;,\; \ldots\ldots \; b_{2p} \;,$$

et la troisième série sera composée des $2p$ nombres qui sont compris dans la série des nombres

$$1\ ,\ 2\ ,\ 3\ ,\ \ldots\ldots\ n-1\ ,$$

sans être compris ni dans la première, ni dans la seconde série. A présent l'équation que nous avons trouvée précédemment, pourra se mettre sous la forme

$$2n=\left\{\begin{array}{l}\left(\sum_{u=1}^{u=p+1}\left(\cos\frac{2a_u\pi}{n}+\sqrt{-1}\sin\frac{2a_u\pi}{n}\right)\right)\left(1+3\sum_{u=1}^{u=p+1}\left(\cos\frac{2a_u\pi}{n}+\sqrt{-1}\sin\frac{2a_u\pi}{n}\right)\right)\\+\left(\sum_{u=1}^{u=p+1}\left(\cos\frac{2b_u\pi}{n}+\sqrt{-1}\sin\frac{2b_u\pi}{n}\right)\right)\left(1+3\sum_{u=1}^{u=p+1}\left(\cos\frac{2b_u\pi}{n}+\sqrt{-1}\sin\frac{2b_u\pi}{n}\right)\right)\\+\left(\sum_{u=1}^{u=p+1}\left(\cos\frac{2c_u\pi}{n}+\sqrt{-1}\sin\frac{2c_u\pi}{n}\right)\right)\left(1+3\sum_{u=1}^{u=p+1}\left(\cos\frac{2c_u\pi}{n}+\sqrt{-1}\sin\frac{2c_u\pi}{n}\right)\right)\end{array}\right.$$

et en posant, pour abréger, les trois équations

$$\sum_{u=1}^{u=p+1}\left(\cos\frac{2a_u\pi}{n}+\sqrt{-1}\sin\frac{2a_u\pi}{n}\right)=A\ ,$$

$$\sum_{u=1}^{u=p+1}\left(\cos\frac{2b_u\pi}{n}+\sqrt{-1}\sin\frac{2b_u\pi}{n}\right)=B\ ,$$

$$\sum_{u=1}^{u=p+1}\left(\cos\frac{2c_u\pi}{n}+\sqrt{-1}\sin\frac{2c_u\pi}{n}\right)=C\ ,$$

on obtiendra

$$2n = A(1+3A) + B(1+3B) + C(1+3C).$$

Mais si l'on exprime par N_2 le nombre des solutions entières, positives et moindres que n, de la congruence

$$x^3 + y^3 + 1 \equiv 0 \quad (\text{mod. } n),$$

on trouvera

$$nN_2 = n^2 + A(1+3A)^2 + B(1+3B)^2 + C(1+3C)^2;$$

et si l'on combine ces deux dernières équations, avec l'équation connue

$$1 + A + B + C = 0,$$

on aura l'équation

$$Z = z^3 + z^2 - \left(\frac{n-1}{3}\right)z - \frac{1}{27}\left(nN_2 + 3 - (n+2)^2 + 9n\right) = 0,$$

qui aura pour racines les trois quantités A, B, C.

On sait que lorsque n est un nombre premier de la forme $6p+1$, l'équation

$$4n = a^2 + 27b^2,$$

pourra toujours être résolue en nombres entiers, mais n'admettra qu'une seule solution; de manière que le nombre n étant donné, a et b seront déterminés, et l'équation $Z = 0$, pourra recevoir l'autre forme

$$Z = z^3 + z^2 - \left(\frac{n-1}{3}\right)z + \frac{1}{27}\left((n-1)^2 - n(n+1\pm a)\right) = 0;$$

et partant en égalant les coefficiens de ces deux équations $Z = 0$, on aura

l'équation

$$N_2 = n \pm a - 2 ,$$

qui exprime un rapport fort singulier entre N_2 et a.

Puisque

$$N_2 = n \pm a - 2 ,$$

et que la valeur de a est comprise entre zéro et $\sqrt{4n - 27}$, le nombre N_2 ne pourra jamais avoir une valeur moindre que

$$n - \sqrt{4n - 27} - 2 ;$$

et par conséquent le nombre N_2 pourra augmenter indéfiniment avec la valeur de n. Il résulte de là que passé une certaine limite, la congruence

$$x^3 + y^3 + 1 \equiv 0 \pmod{n} ,$$

sera toujours résoluble sans faire ni x ni y, divisible par n.

Une autre conséquence assez importante que l'on déduit de l'analyse précédente, c'est que lorsqu'on aura déterminé le nombre N_2 des solutions entières, positives et moindres que n, de la congruence

$$x^3 + y^3 + 1 \equiv 0 \pmod{n} ,$$

on trouvera le nombre N_3 des solutions entières positives et moindres que n, de la congruence

$$x^3 + y^3 + u^3 + 1 \equiv 0 \pmod{n} ,$$

par les formules

$$n N_3 = n^3 + A(1 + 3A)^3 + B(1 + 3B)^3 + C(1 + 3C)^3 ;$$

$$A + B + C = S_1 ; \quad A^2 + B^2 + C^2 = S_2 ;$$

$$A^3 + B^3 + C^3 = S_3 ; \quad A^4 + B^4 + C^4 = S_4 ;$$

$$S_4 + S_3 - \left(\frac{n-1}{3}\right) S_2 + \frac{1}{27}\left((n+2)^2 - 9n - n N_2 - 3\right) S_1 = 0 ;$$

les quantités S_1, S_2, S_3, ayant été déjà déterminées lorsqu'on a formé l'équation $Z = 0$. En général étant donné le nombre N_2, on pourra déterminer le nombre des solutions d'une congruence du troisième degré, contenant un nombre quelconque d'inconnues et ayant des coefficiens quelconques, pourvu qu'elle conserve le même module n.

En faisant $n = 7$, on trouve $a = 1$, $N_2 = 7 - 2 + 1 = 6$; et la congruence

$$x^3 + y^3 + 1 \equiv 0 \quad (\text{mod. } 7),$$

aura toujours six solutions; ce qui il est aisé de vérifier.

Maintenant soit n un nombre premier de la forme $6p + 1$, et tel que l'on ait l'équation

$$4n = a^2 + 27x^2,$$

dans laquelle a est un nombre entier connu, et x un nombre entier indéterminé, mais tel qu'il satisfasse à la condition que n soit un nombre premier de la forme $6p + 1$; il est clair que le nombre des solutions de la congruence

$$z^3 + y^3 + 1 \equiv 0 \quad (\text{mod. } n),$$

sera toujours $n \pm a - 2$, indépendemment de la valeur de x. Ainsi lorsqu'il s'agit des congruences du troisième degré, il ne suffit plus, pour trouver le nombre de leurs solutions, de connaître la forme linéaire des nombres premiers qui servent de module, mais il faut connaître aussi l'un des nombres de la forme quadratique à laquelle ces modules peuvent se réduire; et l'on doit observer qu'à l'aide de la relation $N_2 = n \pm a - 2$, on pourra toujours assigner la valeur de a de manière que N_2 ait une valeur d'une forme donnée; quoiqu'il y ait certaines valeurs que N_2 ne pourra jamais prendre: ainsi on ne pourra jamais avoir les équations

$$N_2 = n \;;\; N_2 = n - 3 \;;\quad \text{etc.}$$

Si l'on exprime toujours par A, B, C, les trois racines de l'équation $Z = 0$, que nous avons trouvée précédemment, on pourra déterminer trois fonctions



entières de x, que l'on exprimera par p, q, r, telles que l'on ait toujours

$$27\,X = 27\left(\frac{x^n - 1}{x - 1}\right) = (p + A\,q + B\,r)(p + B\,q + C\,r)(p + C\,q + A\,r) = 0.$$

Maintenant si l'on effectue les multiplications, et que l'on opère les réductions nécessaires, on trouvera

$$27\,n = \begin{cases} p^3 - p^2(q+r) - \frac{p}{3}\left((n-1)q^2 - (n+2)qr + (n-1)r^2\right) \\ -\frac{q^3}{27}\left((n-1)^2 - n(n+1\pm a)\right) \\ +\frac{q^2 r}{2}\left(\frac{(n+2)(n-1)}{9} \pm nb + \frac{(4-n)(n+1\pm a)}{3\,.\,9}\right) \\ +\frac{q r^2}{2}\left(\frac{(n+2)(n-1)}{9} \mp nb + \frac{(4-n)(n+1\pm a)}{3\,.\,9}\right) \\ -\frac{r^3}{27}\left((n-1)^2 - n(n+1\pm a)\right) \end{cases}$$

en supposant toujours $4\,n = a^2 + 27\,b^2$. Et cette équation offrira le premier exemple d'une forme cubique a trois inconnues à laquelle on pourra réduire un nombre premier quelconque n, de la forme $6p + 1$. On voit que l'on pourrait faire

$$\pm a = N_2 + 2 - n \;\; ; \;\; \pm b = \sqrt{\frac{4\,n - (N_2 + 2 - n)^2}{27}} \;\; ;$$

dans la formule précédente, et elle prendrait alors une autre forme.

L'analyse que nous venons d'exposer fournit le théorème suivant. Lorsque $nt + 1$ est un nombre premier quelconque, et que n est un nombre premier de

la forme $6p + 1$, la congruence du troisième degré à deux inconnues

$$\left.\begin{array}{r} z^3 - z^2(u+1) - \frac{z}{3}\Big((n-1)u^2 - (n+2)u + n - 1\Big) - \frac{u^3}{27}\Big((n-1)^2 - n(n+1 \pm a)\Big) \\ + \frac{u^2}{2}\left(\frac{(n+2)(n+1)}{9} \pm nb + \frac{(4-n)(n+1 \pm a)}{3 \cdot 9}\right) \\ + \frac{u}{2}\left(\frac{(n+2)(n+1)}{9} \mp nb + \frac{(4-n)(n+1 \mp a)}{3 \cdot 9}\right) \\ - \frac{1}{27}\Big((n-1)^2 - n(n+1 \pm a)\Big) \end{array}\right\} \equiv 0 \ (\text{mod. } nt+1),$$

sera toujours résoluble.

On pourrait déduire de ce théorème, de la relation $N_2 = n \pm a - 2$, et de quelques autres propositions que nous omettons ici, un grand nombre de propriétés nouvelles des résidus cubiques des nombres premiers qui ont la forme $6p + 1$; mais nous ne pouvons pas les exposer dans ce mémoire.

Cependant nous fairons observer que puisque l'on a toujours $a^2 < 4n$, l'équation, que nous avons déjà trouvée,

$$Z = z^3 + z^2 - \left(\frac{n-1}{3}\right) z - \frac{1}{27}\Big((3 \pm a)\, n - 1\Big) = 0,$$

tombera dans le cas irréductible, et que par conséquent ses trois racines, que nous avons nommées A, B, C, seront toujours réelles; d'où il résulte que lorsque c est un nombre entier quelconque, et que n est un nombre premier de la forme $6p + 1$, on aura toujours l'équation

$$\sum_{x=0}^{x=n} \sin \frac{2cx^3\pi}{n} = 0 .$$

On trouvera de même en général

$$\sum_{x=0}^{x=n} \sin \frac{2cx^m\pi}{n} = 0 ,$$

toutes les fois que m sera un nombre impair, et que n sera un nombre premier; c étant d'ailleurs un nombre entier quelconque.

Supposons maintenant que n soit un nombre premier de la forme $8m+1$; on sait que l'on pourra toujours résoudre l'équation

$$n = a^2 + 16 b^2 ,$$

et qu'elle n'aura qu'une seule solution. Si l'on cherche le nombre des solutions entières, positives et moindres que n, des congruences

$$x^4+1 \equiv 0 \ (\text{mod.}\, n) , \ x^4+y^4+1 \equiv 0 \ (\text{mod.}\, n) , \ x^4+y^4+u^4+1 \equiv 0 \ (\text{mod.}\, n) ,$$

on sait que la première de ces trois congruences aura quatre solutions, que la seconde en aura un nombre N_2, et que la troisième en aura un nombre N_3; N_2 et N_3, étant deux nombres entiers inconnus. A présent si l'on décompose la série des nombres

$$1 , 2 , 3 , \ldots\ldots . n-1 ,$$

en quatre séries, de la même manière que nous avons décomposé la suite

$$1 , 2 , 3 , \ldots\ldots . n-1 ,$$

en trois séries, quand il s'agissait des congruences du troisième degré, on aura,

après les réductions convenables, les équations

$$1 + A + B + C + D = 0 ;$$

$$4n = n + A(1 + 4A) + B(1 + 4B) + C(1 + 4C) + D(1 + 4D) ,$$

$$nN_2 = n^2 + A(1 + 4A)^2 + B(1 + 4B)^2 + C(1 + 4C)^2 + D(1 + 4D)^2 ,$$

$$nN_3 = n^3 + A(1 + 4A)^3 + B(1 + 4B)^3 + C(1 + 4C)^3 + D(1 + 4D)^3 ,$$

qui serviront à former l'autre équation

$$Z = z^4 + z^3 - 3mz^2 + \varphi(N_2)z + F(N_2, N_3) = 0 ,$$

qui aura pour racines les quatre quantités

$$A , B , C , D ,$$

et dans laquelle le cofficient $\varphi(N_2)$ exprime une fonction de N_2, et le coefficient $F(N_2, N_3)$ représente une fonction de N_2 et N_3 ; fonctions qu'il sera très-facile de déterminer en effectuant le calcul. Mais comme l'on a aussi par l'équation

$$n = a^2 + 16b^2 ,$$

l'autre équation

$$Z = z^4 + z^3 - 3mz^2 + \left(4m^2 - \frac{n(4m+1\pm a)}{8}\right)z + \frac{1}{4}m^2 - n\left(\frac{m}{2} - \frac{4m+1\pm a}{8}\right) = 0 ;$$

on trouvera d'abord, en égalant ces deux équations $Z = 0$, une équation entre N_2 et a, et puis une autre équation entre N_3 et a, ce qui donnera une équation entre N_2 et N_3 ; d'où il résulte que lorsqu'on connait le nombre des solutions de la congruence à deux inconnues

$$x^4 + y^4 + 1 \equiv 0 \pmod{n} ,$$

on aura tout de suite le nombre des solutions de la congrnence à trois inconnues

$$x^4 + y^4 + u^4 + 1 \equiv 0 \pmod{n} ,$$

et par suite le nombre des solutions d'une congruence du quatrième degré, conteuant un nombre quelconque d'inconnues, pourvu que le module n soit toujours un nombre premier de la forme $8m + 1$. On aurait pu établir *à priori* le rapport qui existe entre N_2 et N_3, en observant que dans les quatre équations qui nous ont servi à déterminer les coefficiens de l'équation

$$Z = z^4 + z^3 - 3m\, z^2 + \varphi(N_2)\, z + F(N_2, N_3) = 0 ,$$

on peut négliger la dernière équation qui contient N_3, puisque la première équation

$$1 + A + B + C + D = 0 ,$$

peut se décomposer dans les deux autres

$$A + B = -\frac{1}{2} \pm \frac{1}{2}\sqrt{n} \; ; \; C + D = -\frac{1}{2} \mp \frac{1}{2}\sqrt{n} \; .$$

Une simplification semblable pourra s'effectuer chaque fois que le degré de la congruence que l'on considère ne sera pas un nombre premier; et l'on voit que dans le cas actuel l'équation $Z = 0$, pourra se décomposer en deux équations du second degré, dont les coefficiens ne contiendront d'autre radical que $\sqrt{n}$.

En effectuant les calculs que nous n'avons fait qu'indiquer, on trouverait (par la comparaison des deux équations du quatrième degré $Z = 0$, que nous avons trouvées précédemment) la relation

$$N_2 = n \pm 6a - 3 \; ;$$

en indiquant toujours par N_2 le nombre des solutions entières, positives et moindres que n, de la congruence

$$x^4 + y^4 + 1 \equiv 0 \pmod{n} \; ;$$

et par a le nombre entier qui est donné par l'équation $n = a^2 + 16b^2$. Il résulte de ce qui précède qu'au delà d'une certaine limite, N_2 ira toujours en croissant. Et en général on pourrait démontrer qu'étant donnée la congruence à deux inconnnes

$$x^n + y^n + 1 \equiv 0 \quad (\text{mod. } p) ,$$

dans laquelle p est un nombre premier quelconque, on pourra toujours assigner une limite de p telle, que passé cette limite le nombre des solutions de cette congruence ira toujours en augmentant. Ce théorème n'est pas sans importance pour parvenir à la démonstration de l'impossibilité de résoudre l'équation

$$u^n + v^n = z^n ,$$

en nombres entiers. Car il prouve que l'on tenterait envain de démontrer cette impossibilité, en voulant établir que si cette équation était résoluble, l'une des inconnues serait divisible par un nombre infini de nombres premiers. Nous faisons cette observation, parceque nous avons motif de croire que plusieurs analystes ont tenté ce genre de démonstration, et puis parceque nous avons vu qu'un géomètre distingué, n'a pu démontrer dans aucun cas le théorème que nous avons découvert, et dont nous avons démontré par une méthode particulière les deux premiers cas.

Ce que nous venons de dire sur les congruences du troisième et du quatrième degré, ne renferme que les premiers élémens d'une théorie très-étendue sur les congruences de tous les degrés, théorie que nous exposerons dans une autre occasion; et nous donnerons ici l'énoncé d'un théorème général sur les congruences de tous les degrés; ce théorème est le suivant.

On peut toujours résoudre la congruence

$$x^n + a_1 y^n + a_2 z^n \ldots\ldots + a_n \equiv 0 \quad (\text{mod. } p) ,$$

qui renferme n inconnues et qui est du degré n; le module p étant d'ailleurs un nombre premier quelconque, et les coefficiens

$$a_1 , \quad a_2 , \quad a_3 , \quad \ldots\ldots \quad a_n ,$$

étant des nombres entiers quelconques non divisibles par p.

On voit que ce théorème renferme comme cas particuliers les deux congruences

$$ax + b \equiv 0 \pmod{p},$$

$$x^2 + ay^2 + b \equiv 0 \pmod{p},$$

qui peuvent toujours se résoudre, lorsque le nombre premier p ne divise ni a ni b.

On passerait des congruences aux équations indéterminées, en observant qu'étant proposé de résoudre en nombres entiers l'équation à plusieurs inconnues

$$\varphi(x, y, z, \ldots\ldots \text{etc.}) = 0,$$

elle pourra se réduire à la congruence

$$\varphi(x, y, z, \ldots\ldots \text{etc.}) \equiv 0 \pmod{u},$$

dans laquelle le module u est un nombre entier indéterminé, ou même une fonction quelconque des inconnues x, y, z, ... etc. On peut résoudre par cette méthode plusieurs équations indéterminées, et même on peut trouver avec facilité les facteurs rationnels d'une équation numérique à une seule inconnue, pourvu que l'on détermine convenablement la forme de la fonction représentée par u. Mais cette méthode exige de longs développemens qui ne sauraient trouver place dans ce mémoire.

Tous les résultats obtenus dans ce mémoire, se trouvent exposés dans deux mémoires présentés en 1823, et en 1825, à l'Académie Royale des Sciences de Paris.

MÉMOIRE

SUR LA RÉSOLUTION DE QUELQUES ÉQUATIONS INDÉTERMINÉES.

INTRODUCTION.

Il existe un grand nombre d'équations indéterminées qui n'admettent qu'un petit nombre de solutions entières: mais quoique dans ce cas le problème devienne beaucoup moins compliqué, que lorsque le nombre des solutions est infini, les géomètres n'ont pas cherché à résoudre par une méthode spéciale le cas le plus simple, comme il paraissait naturel de le tenter. En généralisant une méthode que nous avons publiée pour la première fois en 1820, nous sommes parvenus à résoudre complètement un grand nombre d'équations indéterminées, algébriques ou transcendantes, de tous les degrés, contenant deux ou un plus grand nombre d'inconnues.

Lorsqu'on doit résoudre en nombres entiers une équations à plusieurs inconnues, si l'on peut trouver des fonctions de ces inconnues, telles que ces fonctions doivent toujours être comprises entre deux limites numériques données, quelle que soit la valeur que l'on attribue aux variables, il sera toujours possible de réduire l'équation proposée à une autre équation, dans laquelle le nombre des inconnues sera égal au nombre des inconnues de l'équation proposée, moins le nombre des fonctions dont on aura déterminé les limites. Ainsi lorsque le nombre de ces fonctions, augmenté de l'unité, sera égal au nombre des inconnues de l'équation proposée, on aura résolu complètement le problème.

Dans le mémoire publié en 1820, nous avons traité aussi des formes cubiques et de celles du quatrième degré, qui se reproduisent lorsqu'elles sont multipliées par des formes semblables. Maintenant nous reprenons la même matière en l'augmentant considérablement, et nous parvenons à démontrer qu'un nombre quelconque rationnel positif, est toujours la somme de quatre cubes positifs

en nombres rationnels. Enfin nous résolvons dans ce mémoire, une classe assez étendue d'équations indéterminées de tous les degrés, dont Lagrange avait considéré les plus simples.

ANALYSE.

Soit proposé de résoudre en nombres entiers l'équation à deux inconnues

$$\left\{\begin{array}{l} Ab^n v^n \pm Aq^n y^n + \mathrm{F}_{n-1}(v,y) + \mathrm{F}_{n-2}(v,y) \ldots\ldots + \mathrm{F}_{n-m}(v,y) \ldots\ldots \\ \qquad \ldots\ldots + \mathrm{F}_2(v,y) + \mathrm{F}_1(v,y) + T \end{array}\right\} = 0\,,$$

dans laquelle $\mathrm{F}_{n-m}(v\,,\,y)$ représente en général un polynome homogène en v et y, du degré $n-m$, à coefficiens rationnels. On pourra d'abord supposer que tous les coefficiens sont entiers, et que l'on cherche seulement les solutions entières et positives; car tous les autres cas se rapportent à celui-ci, en réduisant les fractions au même dénominateur, et en changeant les signes des variables lorsque cela est nécessaire. Puis on mettra l'équation proposée sous la forme

$$\left\{\begin{array}{l} Ab^n v^n + Bv^{n-1} + v^{n-2}(a+by) + v^{n-3}(a_1 + b_1 y + c_1 y^2) \\ \ldots\ldots\ldots\ldots + v(a_m + b_m y + c_m y^2 \ldots\ldots + p_m y^{n-2}) \\ \qquad \pm Aq^n y^n + Gy^{n-1} + Hy^{n-2} \ldots\ldots + Sy + T = 0 \end{array}\right\} = 0\,;$$

et en multipliant tous les termes de cette équation par $q^n\,b^n$, et en faisant $qy = z$, $bv = x$, on la transformera dans la suivante

$$\left\{\begin{array}{l} Ab^n q^n x^n + Bq^n b x^{n-1} + b^2 x^{n-2}(aq^n + bq^{n-1}z) + b^3 x^{n-3}(a_1 q^n + b_1 q^{n-1} z + c_1 q^{n-2} z^2) \\ \ldots\ldots + b^{n-1} x(a_m q^n + b_m q^{n-1} z \ldots + p_m q^2 z^{n-2}) \pm Ab^n q^n z^n + Gqb^n z^{n-1} \ldots + Tq^n b^n \end{array}\right\} = 0\,,$$

dans laquelle les coefficiens de x^n et de y^n, seront égaux: si à présent l'on suppose $x > z$, et que l'on fasse $x = z + u$, on aura, en développant,

$$(44) \ldots \left\{ \begin{array}{c} A b^n q^n \left((z+u)^n \pm z^n\right) + B q^n b (z+u)^{n-1} + b^2 (a q^n + b q^{n-1} z)(z+u)^{n-2} \\ \ldots\ldots + G q b^n z^{n-1} \ldots\ldots + T q^n b^n \end{array} \right\} = 0 .$$

Maintenant le premier terme de cette équation, est un polynome homogène du degré n, en z et u, ayant tous ses coefficiens positifs; et tous les autres termes sont tels, que les mêmes puissances de z, qui dans le premier terme sont multipliées par des puissances données de u, seront multipliées dans les autres termes par des puissances moindres de u. De sorte que l'on pourra toujours trouver une valeur entière et positive de $u = L$, telle qu'en faisant $u = L + \delta$, (δ étant un nombre quelconque positif) tous les coefficiens de z, dans l'équation (44), restent toujours positifs; et comme par supposition z ne peut avoir que des valeurs positives, l'équation (44) dans laquelle on a fait $u > L$, ne saurait subsister. Par conséquent on devra faire

$$u = 0 \ , \quad u = 1 \ , \quad u = 2 \ , \quad \ldots\ldots u = L \ ;$$

et en substituant successivement ces valeurs dans l'équation (44) on aura une série de $L + 1$ équations à une seule inconnue, dont les facteurs rationnels, s'il en existe, fourniront toutes les valeurs positives de z qui résolvent l'équation (44).

Nous avons supposé $x > z$, si l'on avait au contraire $z > x$, on fairait $z = x + u_1$, et l'on obtiendrait la limite de u_1 de la même manière que l'on a trouvé la limite de u

De cette manière nous avons trouvé toutes les solutions entières et positives de l'équation proposée; pour trouver les solutions entières et négatives, l'on n'aurait qu'à changer les signes des variables, comme nous l'avons déjà indiqué.

Soit proposée l'équation à deux inconnues

$$f(x, y) \cdot F(x, y) = F_1(x, y),$$

on pourra toujours en avoir toutes les solutions entières et positives, lorsque les trois fonctions

$$f(x, y), \quad F(x, y), \quad F_1(x, y),$$

étant rationnelles et entières, les signes des termes qui contiennent les plus grandes puissances de x et de y dans le polynome $f(x, y)$ seront tous égaux, et que les exposans de ces puissances ne seront pas moindres que ceux des puissances les plus élevées contenues dans le polynome $F_1(x, y)$; et on aura de même toutes les solutions entières et négatives, lorsqu'en changeant les signes des inconnues, les puissances les plus élevées de x et de y, comprises dans le polynome $f(x, y)$, seront toutes du même signe; ou du moins pourront se réduire, à l'aide de quelque artifice de calcul, à n'avoir que le même signe. En effet, en faisant

$$x = x_1 + u, \quad y = y_1 + t,$$

la fonction $f(x, y)$, se réduira aisément à avoir tous ses termes du même signe, et l'on déterminera les limites de u et de t, qui deviendront de cette manière des coefficiens numériques: alors on pourra trouver un nombre entier et positif A, tel que l'on ait toujours, pour des valeurs entières et positives des inconnues, en prenant $f(x_1, y_1)$ avec tous les termes positifs, l'inégalité

$$(A + r) f(x_1, y_1) > F_1(x_1, y_1);$$

(r étant une quantité positive quelconque) et l'on pourra toujours déterminer un autre nombre entier B tel que l'on ait (pour des valeurs entières et positives des inconnues, et en prenant encore la fonction $f(x_1, y_1)$ positivement) l'inégalité

$$(B - r) f(x_1, y_1) < F_1(x_1, y_1);$$

d'où il résulte que $F_1(x_1, y_1)$, ne pourra avoir qu'un nombre limité de valeurs comprises entre B et A ; de manière qu'en faisant successivement

$$F_1(x_1, y_1) = B, \quad F_1(x_1, y_1) = B + 1, \quad \ldots\ldots \; F_1(x_1, y_1) = A,$$

on aura un nombre $A - B + 1$ d'équations qui, étant combinées avec l'équation proposée, fourniront par l'élimination un nombre égal d'équations à une seule inconnue, d'où l'on tirera toutes les solutions de l'équation proposée.

Il est facile d'appliquer ce principe aux équations contenant plus de deux inconnues, de la forme

$$f(x, y, z, \ldots \text{etc.}) f_1(x, y, z, \ldots \text{etc.}) \ldots f_n(x, y, z, \ldots \text{etc.}) = F(x, y, z, \ldots \text{etc.}),$$

pourvu que le nombre des facteurs qui composent le premier membre soit égal au moins au nombre des inconnues; et l'on voit que la forme des fonctions

$$f, \; f_1, \; \ldots\ldots \; f_n, \; F,$$

peut être algébrique ou transcendante.

Soit proposé, par exemple, de trouver toutes les solutions entières et positives de l'équation transcendante

$$x^y (x^2 - y^2) = 2y^3,$$

que l'on pourra réduire à la forme suivante

$$(x^2 - y^2)\left(1 + y \log x + \frac{y^2}{1 \cdot 2} (\log x)^2 + \frac{y^3}{1 \cdot 2 \cdot 3} (\log x)^3 \ldots\ldots + \text{etc.}\right) = 2y^3;$$

il est évident que les deux inégalités

$$x > 2, \quad x^2 - y^2 > 11,$$

ne pourront pas subsister ensemble, parceque si elles pouvaient exister en même tems, le premier membre de cette équation serait toujours plus grand que le second, tant que les nombres x et y resteraient positifs. Alors il faudra que l'on ait l'une des équations

$$x = 0, \; x = 1, \; x = 2; \; x^2 - y^2 = 0, \; x^2 - y^2 = 1,$$

$$x^2 - y^2 = 2, \; x^2 - y^2 = 3, \; x^2 - y^2 = 4, \; x^2 - y^2 = 5, \; x^2 - y^2 = 6,$$

$$x^2 - y^2 = 7, \; x^2 - y^2 = 8, \; x^2 - y^2 = 9, \; x^2 - y^2 = 10, \; x^2 - y^2 = 11.$$

Mais les équations

$$x^2 - y^2 = 2 \quad , \quad x^2 - y^2 = 6 \quad , \quad x^2 - y^2 = 10 \quad ,$$

ne peuvent avoir aucune solution entière; et parmi les 12 équations qui restent, il n'y a que les deux équations $x = 0$, $x^2 - y^2 = 0$, qui étant combinées avec l'équation proposée servent à la résoudre: on déduit de là que l'équation

$$x^y (x^2 - y^2) = 2y^3 \quad ,$$

ne peut se résoudre en nombres entiers et positifs, qu'en faisant $x = 0$, $y = 0$. On pourrait, de la même manière trouver les solutions entières et négatives de l'équation proposée.

L'équation

$$A b^n x^n - A q^n y^n = \mathrm{F}_{n-1}(x , y) + \mathrm{F}_{n-2}(x , y) \ldots\ldots + T \quad ,$$

qui est semblable à celle que nous avons déjà considérée, peut se résoudre assez facilement par la méthode que nous venons d'exposer; car cette équation peut se réduire à la forme

$$f(x , y) \cdot F(x , y) = F_1(x , y) \quad ,$$

en faisant

$$F(x , y) = A(bx - qy) \; ; \; f(x , y) = b^{n-1} x^{n-1} + b^{n-2} x^{n-2} q y \ldots . + q^{n-1} y^{n-1} \quad ;$$

$$F_1 (x , y) = \mathrm{F}_{n-1} (x , y) + \mathrm{F}_{n-2} (x , y) \ldots\ldots + T \quad ;$$

et on pourra de cette manière trouver toutes les solutions entières et positives de l'équation proposée. Si l'on voulait résoudre l'équation

$$A b^n x^n + A q^n y^n = \mathrm{F}_{n-1} (x , y) + \mathrm{F}_{n-2} (x , y) \ldots\ldots + T \, ,$$

il faudrait multiplier tous ses termes par $b^n x^n - q^n y^n$, afin de rendre le

premier membre décomposable dans les deux facteurs

$$A(bx - qy) \quad , \quad b^{2n-1} x^{2n-1} + b^{2n-2} x^{2n-2} qy \ldots . + q^{2n-1} y^{2n-1} \quad ,$$

le second desquels a tous ses termes positifs. De cette manière l'on trouve toutes les solutions entières et positives; les solutions entières et négatives, s'obtiennent en changeant les signes des variables.

En général, étant proposé de résoudre en nombres entiers une équation à n inconnues, si l'on peut former, avec ces mêmes inconnues, m fonctions entières, chacune desquelles, pour des valeurs quelconques des inconnues, doive être moindre que $L + 1$, et plus grande que L_1, (L et L_1 étant deux nombres entiers) en égalant successivement chacune de ces fonctions aux nombres

$$L_1 + 1 \quad , \quad L_1 + 2 \quad , \quad \ldots \ldots \quad L \quad ,$$

on aura $m\,(L - L_1)$ équations; et les solutions entières de l'équation proposée, devront se trouver parmi les racines entières de ces dernières équations; et si la nature des fonctions que l'on a trouvées est telle, qu'en combinant les divers systèmes d'équations qui en résultent avec l'équation proposée on puisse éliminer m inconnues, on obtiendra une équation plus simple qui ne contiendra que $n - m$ inconnues; et lorsque $m = n - 1$, l'équation proposée sera résolue complètement

Soit proposé de résoudre en nombres entiers l'équation à coefficiens rationnels

$$(45) \ldots \ldots \quad a^2 x^4 + bx^3 + cx^2 + dx + e = z^2 \;;$$

on pourra toujours supposer que les coefficiens de cette équation sont entiers; car s'ils ne l'étaient pas, ils deviendraient tels en les réduisant au même dénominateur, et en multipliant toute l'équation par le carré de ce dénominateur. De plus on supposera que les inconnues x et z, sont positives; car si elles sont négatives, on pourra changer leurs signes et les rendre positives, et l'on admettra que tous les coefficiens du premier membre sont positifs; car s'il y en avait de négatifs, on les rendrait tous positifs en posant $x = x_1 + h$, et en déterminant h convenablement.

Maintenant si l'on multiplie par $4\,a^2$ tous les termes de l'équation (45), et

que l'on fasse $4a^2z^2 = (2a^2x^2 + bx + v)^2$, on aura en développant

$$\left.\begin{aligned} &4a^4x^4 + 4a^2bx^3 + 4a^2cx^2 + 4a^2dx + 4a^2e \\ &-4a^4x^4 - 4a^2bx^3 - (4a^2v + b^2)x^2 - 2bvx - v^2 \end{aligned}\right\} = 0,$$

et partant

$$(46)\ldots(4a^2v + b^2 - 4a^2c)x^2 + (2bv - 4a^2d)x + v^2 - 4a^2e = 0.$$

Dans cette dernière équation v peut être positif ou négatif; si on le suppose positif, il ne pourra jamais surpasser un nombre L qui, substitué pour v dans l'équation (46), rendrait tous ses termes positifs; alors on devra faire successivement

$$v = 0\ ,\ 1\ ,\ 2\ ,\ 3\ ,\ \ldots\ldots\ L - 1\ ,$$

et on obtiendra par l'élimination toutes les solutions entières et positives qui correspondent à l'hypothèse de v positif. Soit v négatif et égal à $-t$, et soit $t < x$; en substituant cette valeur dans l'équation (46), elle deviendra

$$(47)\ldots(b^2 - 4a^2c - 4a^2t)x^2 + (-2bt - 4a^2d)x + (t^2 - 4a^2e) = 0:$$

maintenant si l'on suppose que s soit la plus petite des valeurs entières de t qui satisfont à l'inégalité

$$4a^2(t + c) > b^2\ ,$$

en substituant $s + \omega$, pour t dans l'équation (47), (ω étant un nombre positif quelconque) on en déduira une autre équation de la forme

$$Ax^2 + Bx + 4a^2c = (s + \omega)^2\ ,$$

qui a tous ses coefficiens positifs, mais qui est absurde parceque l'on a par supposition

$$x^2 > t^2 = (s + \omega)^2 .$$

S'il existe donc une valeur de v, négative et moindre que x, qui satisfasse à l'équation proposée, elle devra se trouver parmi les nombres

$$-1 , -2 , -3 , \ldots\ldots -(s-1) .$$

Si dans l'équation (46), on a $v = -u$ et $u > x$, en divisant u par x, on trouvera le quotient n et le reste $r < x$, et en posant

$$4\,a^2 z^2 = (2\,a^2 x^2 + bx - nx - r)^2 = \big(2\,a^2 x^2 + (b-n)\,x - r\big)^2,$$

on obtiendra

$$\left\{\begin{array}{c} 4\,a^4 x^4 + 4\,a^2 b\,x^3 + 4\,a^2 c\,x^2 + 4\,a^2 d\,x + 4\,a^2 e \\ -4\,a^4 x^4 - 4\,a^2 (b-n)\,x^3 + \big(4\,a^2 r - (b-n)^2\big)\,x^2 + 2\,(b-n)\,r\,x - r^2 \end{array}\right\} =$$

$$4\,a^2 n\,x^3 + \big(4\,a^2 r + 4\,a^2 c - (b-n)^2\big)\,x^2 + \big(2\,(b-n)\,r + 4\,a^2 d\big)\,x + 4\,a^2 e - r^2 = 0 ;$$

mais puisque $4\,a^2 z^2 > 4\,a^4 x^4$, on aura toujours $b > n$, et par conséquent on faira successivement

$$n = 1 , 2 , 3 , \ldots\ldots b-1 ;$$

et en substituant toutes ces valeurs dans l'équation précédente, on déterminera, comme auparavant, la limite de r.

De cette manière nous avons réduit l'équation proposée à dépendre d'un nombre donné d'équations à une seule inconnue, dont on sait trouver tous les facteurs rationnels.

Soit proposé; par exemple, de résoudre en nombres entiers et positifs l'équation à deux inconnues

$$x^4 + 4x^3 + 11 = z^2 ;$$

en faisant $z = x^2 + 2x + r$, on aura, après les réductions,

$$(4 + 2r)x^2 + 4rx + r^2 - 11 = 0 ;$$

si r est un nombre positif, on voit qu'on ne saurait avoir $r > 3$; si r est égal à un nombre négatif $-p$ et que l'on ait $p < x$, on obtiendra

$$(4 - 2p)x^2 - 4px + p^2 - 11 = 0 ;$$

et en faisant $p = 3$, ou $p > 3$, on trouvera une équation de la forme

$$ax^2 + bx + 11 = p^2 ,$$

qui est absurde parceque par supposition $x^2 > p^2$.

Lorsque r est un nombre négatif, et que l'on $a - r > x$, on faira $r = -(x + t)$; en supposant $-t < x$, et on obtiendra

$$x^4 + 4x^3 + 11 = (x^2 + x - t)^2$$

et par suite

$$2x^3 + (2t - 1)x^2 + 2tx + 11 = t^2 ,$$

et puisque $x^2 > t^2$, on ne pourra pas avoir $t > 0$.

Il serait absurde de supposer $r = -(nx + t)$, et $n > 1$, parceque l'on aurait alors l'équation

$$z^2 = (x^2 - A)^2 < x^4 ,$$

qui ne saurait jamais s'accorder avec l'autre

$$z^2 = x^4 + 4x^3 + 11 > x^4 .$$

Par conséquent l'on obtiendra le système suivant d'équations

$$z = x^2 + 2x + 1\ ,\quad z = x^2 + 2x + 2\ ,\quad z = x^2 + 2x\ ,$$

$$z = x^2 + 2x + 3\ ,\quad z = x^2 + 2x - 1\ ,\quad z = x^2 + \quad x\ ,$$

qui étant combinées avec l'équation proposée doivent servir à déterminer les valeurs des inconnnes. Maintenant si l'on effectue les éliminations, on ne trouve que les valeur $x = 1$, $z = 4$, qui résolvent l'équation proposée, et qui donnent

$$1^4 + 4 \times 1^3 + 11 = 4^2\ .$$

L'équation que nous venons de traiter sert à résoudre l'autre

$$(48)\ldots\ Ax^2 + (By^2 + Cy + D)x + Ey^3 + Fy^2 + Gy + H = 0\ ,$$

lorsque B n'est point égal à zéro; en effet on trouve l'expression

$$x = \frac{-(By^2 + Cy + D) \pm \sqrt{(By^2 + Cy^2 + D) - 4A(Ey^3 + Fy^2 + Gy + H)}}{2A}\ ,$$

dans laquelle la quantité comprise sous le signe radical doit satisfaire à une équation de la forme

$$z^2 = a^2y^4 + by^3 + cy^2 + dy + e\ ;$$

et lorsqu'on aura obtenu toutes les solutions de cette équation, on aura résolu complètement l'équation proposée.

Si dans l'équation (48), l'on fait

$$y = x + t\ ,\quad H = a\ ,\quad G = e\ ,\quad F = f\ ,\quad E = g\ ,$$

$$D + g = b\ ,\quad F = c\ ,\quad B + E = d\ ,\quad E + 2F = h\ ,$$

on la transformera, après les substitutions, dans la suivante

$$0 = a + bx + cx^2 + dx^3 + et + ft^2 + gt^3 + hxt + (d + 2g)xt^2 + (2d + g)x^2t\ ,$$



qui est assez générale, et dont on pourra trouver toutes les solutions entières.

Si au lieu de l'équation (48) on avait considéré la suivante

$$Ax^2+(B+Cy\ldots+Dy^n+Ey^{n+1}\ldots+Fy^{n+p})x+Gy^{2n-1}+Hy^{2n-2}\ldots+I=0,$$

on aurait pu la résoudre de la même manière, pourvu que tous les coefficiens D, E, ... F, ne s'évanouissent pas à la fois; et l'on en aurait déduit de nouvelles transformées plus générales que celle que nous venons de trouver; car la méthode dont nous avons fait usage pour résoudre l'équation (45), peut s'appliquer également à l'autre plus générale

$$Aa^n x^{mn} + bx^{mn-1} + cx^{mn-2} \ldots\ldots + px + q = Ac^n z^n .$$

On a déjà vu que par $F_n(x, y)$, nous désignons une fonction homogène, rationnelle et entière, du degré n, entre x et y; en généralisant cette notation, nous représenterons dans la suite par $F_n(x, y, z, \ldots\ldots$ etc.$)$, une fonction homogène, rationnelle et entière, du degré n, entre les inconnues

$$x, \quad y, \quad z, \quad \ldots\ldots \text{ etc.}$$

Maintenant, étant donnée l'equation

$$F_2(x, y) + F_1(x, y) + f = 0,$$

si l'on peut trouver une solution rationnelle de celle-ci

$$F_2(x, y) = ax^2 + bxy + cy^2 = 0,$$

la première sera résoluble aussi en nombres rationnels. En effet, si les valeurs $x = m$, $y = n$, satisfont à l'équation $F_2(x, y) = 0$, en faisant

$$x = mp + q, \quad y = np + r,$$

et en substituant ces valeurs dans l'équation

$$F_2(x, y) + F_1(x, y) + f = ax^2 + bxy + cy^2 + dx + ey + f = 0,$$

on aura

$$\left\{\begin{array}{c}(am^2+bmr+cn^2)\,p^2+\left(2\,amq+b\,(mr+nq)+2\,cnr+dm+en\right)p\\ +\,aq^2+bqr+cr^2+dq+er+f\end{array}\right\}=0\,;$$

et puisque par hypothèse on a $am^2+bmn+cn^2=0$, on obtiendra l'équation

$$p=-\frac{aq^2+bqr+cr^2+dq+er+f}{2\,amq+bnq+bmr+2cnr+dm+en},$$

dans laquelle les inconnues q, r, peuvent prendre des valeurs rationnelles quelconques, et en substituant cette valeur de p, dans les valeurs de x et de y, on obtiendra toutes les solutions rationelles de l'équation proposée.

Il est clair que la même chose arriverait si l'on avait l'équation

$$(49)\ldots\ F_2(x,y,z,\ldots\text{ etc.})+F_1(x,y,z,\ldots\text{ etc.})+f=0\,;$$

qui renferme un nombre quelconque d'inconnues. Et il faut observer qu'étant donnée une solution $x=l$, $y=m$, $z=n$, ... etc., en nombres rationnels, de l'équation

$$F_2(x\,,\,y\,,\,z\,,\,\ldots\ldots\text{ etc.})=0\,,$$

on peut trouver toutes les solutions rationnelles de l'équation (49) en faisant

$$x=lp+q\,,\quad y=mp+r\,,\quad z=np+s\,,\ \ldots\ \text{etc.}\,,$$

(les quantités q, r, s, ... etc., étant des nombres rationnels quelconques) et l'on voit que ces solutions seront toujours en nombre infini.

Par exemple, on sait qu'un nombre entier quelconque A est toujours la

somme de quatre carrés en nombres entiers, on aura par conséquent

$$A = a^2 + b^2 + c^2 + d^2 \;;$$

mais si l'on voulait connaître toutes les solutions rationnelles de l'équation

$$A = x^2 + u^2 + y^2 + z^2 \;,$$

on fairait

$$A p^2 = (ap + q)^2 + (bp + r)^2 + (cp + s)^2 + (dp + t)^2 \;,$$

et l'on aurait

$$p = - \frac{q^2 + r^2 + s^2 + t^2}{2\,(aq + br + cs + dt)} \;,$$

et la formule

$$A = \left(a + \frac{q}{p}\right)^2 + \left(b + \frac{r}{p}\right)^2 + \left(c + \frac{s}{p}\right)^2 + \left(d + \frac{t}{s}\right)^2 \;,$$

(dans laquelle on peut donner à q, r, s, t, des valeurs rationnelles quelconques) exprimera toutes les manières de décomposer le nombre A en quatre carrés rationnels.

Il faut observer qu'étant donnée l'équation

$$(50)\ldots ax^2 + bxy + cy^2 + dxz + eyz + fz^2 + gx + hy + iz + k = 0 \;,$$

si l'équation

$$ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = 0 \;,$$

est satisfaite en faisant $x = n$, $y = r$, $z = m$; on substituera dans

l'équation proposée les valeurs

$$x = np + q \quad , \quad y = rp + s \quad , \quad z = mp + t \quad ,$$

et on aura

$$p = -\frac{aq^2 + bqs + cs^2 + dqt + est + ft^2 + gq + hs + it + k}{2(anq+crs+fmt)+b(sn+qr)+d(nt+qm)+e(rt+sm)+gn+hr+im} \, ,$$

où il faut observer que lorsqu'on pourra résoudre en nombres entiers l'équation

$$(2an+br+dm)q+(2cr+bn+em)s\pm(2fm+dn+er)t+gn+hr+im=1 \, ,$$

qui contient les trois inconnues q , s , t , on pourra résoudre aussi l'équation (50) en nombres entiers, d'une infinité de manières.

Si l'équation proposée se réduisait à la forme

$$ax^2 + cy^2 + fz^2 + k = 0 \, ,$$

pour tâcher de la résoudre en nombres entiers il faudrait faire

$$anq + crs + fmt = \pm 1 \, .$$

Cependant il y a des cas dans lesquels l'équation proposée ne saurait être résolue en nombres entiers, quoiqu' elle puisse avoir une infinité de solutions fractionnaires.

Lagrange a démontré que lorsqu'on multiplie ensemble les deux formules

$$x^2 - ay^2 - bz^2 + abu^2 = F \, ,$$
$$X^2 - aY^2 - bZ^2 + abU^2 = F_1 \, ,$$

on aura toujours l'équation

$$FF_1 = A^2 - aB^2 - bC^2 + abD^2 \, ,$$

dans laquelle les quantités A , B , C , D , sont déterminées; maintenant si

l'on fait

$$p = -\frac{x_1^2 - a y_1^2 - a z_1^2 + a b u_1^2}{2 (A x_1 - a B y_1 - b C z_1 + a b D u_1)}$$

(les quantités x_1, y_1, z_1, u_1, étant des nombres rationnels quelconques) on aura

$$F F_1 = \left(A + \frac{x_1}{p}\right)^2 - a\left(B + \frac{y_1}{p}\right)^2 - b\left(C + \frac{z_1}{p}\right)^2 + ab\left(D + \frac{u_1}{p}\right)^2,$$

et cette formule comprendra toutes les manières dont on peut réduire le produit $F F_1$ à la forme

$$n^2 - a q^2 - b r^2 + a b s^2 .$$

Notre analyse fournit beaucoup de nouvelles formules semblables, car en faisant

$$F = \mathrm{F}_2(x, y, z, u, \ldots\ldots \text{etc.}) + A,$$

$$F_1 = \mathrm{F}_2(X, Y, Z, U, \ldots\ldots \text{etc.}) + A,$$

on trouvera aisément que l'on a toujours

$$F F_1 = \mathrm{F}_2(p, q, r, s, \ldots\ldots \text{etc.}) + A,$$

(les quantités $p, q, r, s, \ldots$ etc., étant des fonctions rationnelles des quantités $A, x, X, y, Y, z, Z, \ldots$ etc.) pourvu que l'on puisse résoudre l'équation

$$\mathrm{F}_2(x_1, y_1, z_1, u_1, \ldots\ldots \text{etc.}) = 0,$$

en nombres rationnels. Ainsi, par exemple, si l'on fait

$$F = x^2 + 41 y^2 - 113 z^2 + a t^4,$$

$$F_1 = X^2 + 41 Y^2 - 113 Z^2 + a T^4,$$

on aura

$$FF_1 = \begin{cases} a\,s^4 + \left(\dfrac{19\,(FF_1 + 113\,r^2 - p^2 - 41\,q^2 - a\,s^4)}{2\,(19\,p + 164\,q - 339\,r)} + p\right)^2 \\ + 41\left(\dfrac{4\,(FF_1 + 113\,r^2 - p^2 - 41\,q^2 - a\,s^4)}{2\,(19\,p + 164\,q - 339\,r)} + q\right)^2 \\ - 113\left(\dfrac{3\,(FF_1 + 113\,r^2 - p^2 - 41\,q^2 - a\,s^4)}{2\,(19\,p + 164\,q - 339\,r)} + r\right)^2 \end{cases}$$

les quantités p , q , r , s , étant des nombres rationnels quelconques.

Ce que nous venons de dire par rapport aux formules du second degré, peut s'appliquer aux équations indéterminées du troisième degré, et si l'équation à deux inconnues

$$F_3\,(x\,,y) = 0 \quad ,$$

est résoluble en nombres rationnels, l'autre

$$F_3\,(x\,,y) + F_2\,(x\,,y) + F_1\,(x\,,y) + k = 0\ ,$$

sera résoluble aussi: en effet étant proposée l'équation

$$(51)\ldots a x^3 + b x^2 y + c x y^2 + d y^3 + e x^2 + f x y + g y^2 + h x + i y + k = 0\ ,$$

si l'on peut trouver deux nombres entiers m , n , tels que l'on ait

$$a m^3 + b m^2 n + c m n^2 + d n^3 = 0\ ,$$

on pourra faire $x = mp + q$, $y = np + r$, et en substituant ces valeurs dans l'équation (51), on aura une équation de la forme

$$(52)\ \ldots\ldots\ldots\ A p^3 + B p^2 + C p + D = 0\ ,$$

dans laquelle

$$A = am^3 + bm^2n + cmn^2 + dn^3 = 0\ ;$$

et si l'on fait $B = 0$, on pourra résoudre l'équation (52) et l'on aura $p = -\frac{D}{C}$;
et en éliminant q entre les équations

$$B = 0\ ,\quad p = -\frac{D}{C}\ ,$$

on obtiendra une équation de la forme

$$p = -F(r)\ ,$$

(dans laquelle $F(r)$ exprime une fonction rationnelle quelconque de r) qui fournira une infinité de solutions de l'équation proposée lorsqu'on donnera à r des valeurs rationnelles quelconques.

Il est clair que l'on parviendrait à un résultat semblable, si l'équation proposée contenait un plus grand nombre d'inconnues ; car si l'équation

$$F_3(x\ ,\ y\ ,\ z\ ,\ u\ ,\ \ldots\ldots \text{etc.}) = 0\ ,$$

peut être résolue en nombres rationnels, l'autre équation

$$F_3(x,y,z,u,\ldots \text{etc.}) + F_2(x,y,z,u,\ldots \text{etc.}) + F_1(x,y,z,u,\ldots \text{etc.}) + f = 0\ ,$$

aura un nombre infini de solutions rationnelles. Maintenant si dans l'équation précédente on fait

$$f = -m\ ,\ F_3(x\ ,y\ ,z\ ,u\ ,\ldots\ldots \text{etc.}) = x^3 + y^3 - z^3 - u^3\ ,$$

$$F_2(x\ ,y\ ,z\ ,u\ ,\ldots\ldots \text{etc.}) = F_1(x\ ,y\ ,z\ ,u\ ,\ldots\ldots \text{etc.}) = 0\ ,$$

(m étant un nombre rationnel quelconque) puisque l'équation

$$x^3 + y^3 - z^3 - u^3 = 0\ ,$$



peut se résoudre en faisant $x = y = z = u$, on pourra résoudre aussi l'équation

$$z^3 + y^3 - z^3 - u^3 = m \quad ,$$

et l'on aura l'identité

$$(52) \ldots m = \left(\frac{m + 6q^3}{6q^2}\right)^3 + \left(\frac{m - 6q^3}{6q^2}\right)^3 - \left(\frac{m}{6p^2}\right)^3 - \left(\frac{m}{6q^2}\right)^3 ,$$

dans laquelle q est un nombre quelconque rationnel. De cette manière l'on a décomposé le nombre rationnel m en quatre cubes rationnels, dont deux seront positifs et deux négatifs. Mais on peut, lorsque m est un nombre positif, réduire le second nombre de cette équation à ne contenir que des cubes positifs, et c'est ce que nous allons prouver à présent.

Supposons q positif et tel que l'on ait $6q^3 < m$; il est clair qu'alors les deux premiers cubes du second nombre de l'équation (52) seront positifs, tandis que les deux autres seront négatifs. De plus dans l'identité

$$(53) \ldots\ldots a^3 - b^3 = a^3\left(\frac{a^3 - 2b^3}{a^3 + b^3}\right)^3 + b^3\left(\frac{2a^3 - b^3}{a^3 + b^3}\right)^3 ,$$

le second membre est la somme de deux cubes positifs lorsqu'on a $a^3 > 2b^3$, car à plus forte raison on aura $2a^3 > b^3$; si l'on fait donc

$$a = \frac{m + 6q^3}{6q^2} \quad , \quad b = \frac{m}{6q^2} \quad ,$$

l'équation (53) se transformera dans la suivante

$$(54) \ldots \left(\frac{m+6q^3}{6q^2}\right)^3 - \left(\frac{m}{6q^2}\right)^3 = \left\{ \begin{array}{l} \left(\frac{m+6q^3}{6q^2}\right)^3 \left(\frac{(m+6q^3)^3 - 2m^3}{(m+6q^3)^3 + m^3}\right)^3 \\ + \left(\frac{m}{6q^2}\right)^3 \left(\frac{2(m+6q^3)^3 - m^3}{(m+6q^3)^3 + m^3}\right)^3 \end{array} \right\}$$

dans laquelle les deux cubes qui composent le second membre seront positifs lorsqu'on aura

$$(m + 6q^3)^3 > 2m^3 .$$

Supposons maintenant que cette inégalité soit satisfaite, et reprenons l'identité (53) en y faisant

$$a = \left(\frac{m + 6q^3}{6q^2}\right)\left(\frac{(m + 6q^3)^3 - 2m^3}{(m + 6q^3)^3 + m^3}\right) , \quad b = \frac{m}{6q^2} ,$$

il clair que nous aurons l'équation

$$(55) \ldots \left(\frac{m + 6q^3}{6q^2}\right)^3\left(\frac{(m + 6q^3)^3 - 2m^3}{(m + 6q^3)^3 + m^3}\right)^3 - \left(\frac{m}{6q^2}\right)^3 =$$

$$\left\{\begin{array}{l} \left(\frac{m+6q^3}{6q^2}\right)^3\left(\frac{(m+6q^3)-2m^3}{(m+6q^3)^3+m^3}\right)^3\left\{\frac{\left(\frac{m+6q^3}{6q^2}\right)^3\left(\frac{(m+6q^3)^3-2m^3}{(m+6q^3)^3+m^3}\right)^3-2\left(\frac{m}{6q^2}\right)^3}{\left(\frac{m+6q^3}{6q^2}\right)^3\left(\frac{(m+6q^3)^3-2m^3}{(m+6q^3)^3+m^3}\right)^3+\left(\frac{m}{6q^2}\right)^3}\right\}^3 \\ \qquad + \left(\frac{m}{6q^2}\right)^3\left\{\frac{2\left(\frac{m+6q^3}{6q^2}\right)^3\left(\frac{(m+6q^3)^3-2m^3}{(m+6q^3)^3+m^3}\right)^3-\left(\frac{m}{6q^2}\right)^3}{\left(\frac{m+6q^3}{6q^2}\right)^3\left(\frac{(m+6q^3)^3-2m^3}{(m+6q^3)^3+m^3}\right)^3+\left(\frac{m}{6q^2}\right)^3}\right\}^3 \end{array}\right\} ,$$

dans laquelle le premier cube du second membre pourra s'écrire de cette manière

$$\left(\frac{m+6q^3}{6q^2}\right)^3\left(\frac{(m+6q^3)^3-2m^3}{(m+6q^3)^3+m^3}\right)^3\left(\frac{(m+6q^3)^3\left((m+6q^3)-2m^3\right)^3-2m^3\left((m+6q^3)^3+m^3\right)^3}{(m+6q^3)^3\left((m+6q^3)^3-2m^3\right)^3+m^3\left((m+6q^3)^3+m^3\right)^3}\right)^3$$

et afin que ce cube soit positif il suffira que l'inégalité

$$(56)\ldots (m+6q^3)^3\left((m+6q^3)^3-2m^3\right)^3 > 2m^3\left((m+6q^3)^3+m^3\right)^3,$$

soit satisfaite; et l'on voit que cette inégalité renferme l'autre

$$(m + 6q^3)^3 > 2m^3,$$

(puisque les deux nombres m et q, sont positifs par supposition) et que lorsque l'inégalité (56) sera satisfaite, le second cube du second membre de l'équation (55) sera positif aussi, puisque si l'inégalité (56) est satisfaite, l'autre

$$2(m+6q^3)^3\left((m+6q^3)-2m^3\right)^3 > m^3\left((m+6q^3)^3+m^3\right)^3,$$

sera satisfaite aussi. Il suffira donc de satisfaire à l'inégalité (56) pour que les deux cubes du second membre de l'équation (54), et les deux cubes du second membre de l'équation (55) soient positifs.

Soit, pour abréger, $6q^3 = z$, l'inégalité (56) deviendra, en extrayant la racine cubique,

$$(z+m)\left((z+m)^3-2m^3\right)-m\left((z+m)^3+m^3\right)\sqrt[3]{2} > 0,$$

d'où l'on déduira, en ordonnant le premier membre par les puissances de z,

$$(57)\ldots z^4+m\left(4-\sqrt[3]{2}\right)z^3+m^2\left(6-3\sqrt[3]{2}\right)z^2+m^3\left(2-3\sqrt[3]{2}\right)z-m^4\left(1+2\sqrt[3]{2}\right)>0.$$

On a supposé $m > 6q^3$, ou bien $m > z$; en faisant donc $m = Az$, on aura $A > 1$, et en substituant cette valeur de m dans l'inégalité (57), on aura, après avoir divisé par z^4; l'autre inégalité

$$1+\left(4-\sqrt[3]{2}\right)A+\left(6-3\sqrt[3]{2}\right)A^2+\left(2-3\sqrt[3]{2}\right)A^3-\left(1+2\sqrt[3]{2}\right)A^4>0,$$

et celle-ci, en y faisant $A = 1 + x$, se transformera dans la suivante

$$(58)\ldots 12 - 9\sqrt[3]{2} + \left(18 - 24\sqrt[3]{2}\right)x + \left(6 - 24\sqrt[3]{2}\right)x^2 - \left(2 + 11\sqrt[3]{2}\right)x^3 - \left(1 + 2\sqrt[3]{2}\right)x^4 > 0,$$

dans laquelle il sera toujours possible de trouver pour x un nombre rationnel positif qui lui satisfasse; en effet puisque l'on a $126 > 100\sqrt[3]{2}$, on aura aussi

$$12 - 9\sqrt[3]{2} > \frac{33}{55},$$

et x devra être un nombre tel que la somme de tous les termes qu'il multiplie dans l'inégalité (58) soit moindre que $\frac{33}{50}$. On faira à cet effet $100\sqrt[3]{2} = 126$, car tous les termes qui sont multipliés par x dans l'inégalité (58) étant négatifs, on ne devra craindre aucune erreur en prenant pour $\sqrt[3]{2}$ un nombre un peu plus grand que la valeur exacte de ce radical. Par cette substitution l'inégalité (58) se transformera dans la suivante

$$33 - 622x - 1212x^2 - 793x^3 - 226x^4 > 0;$$

d'où l'on déduira, en faisant $x = \frac{1}{y}$,

$$y^4 - \frac{612}{33}y^3 - \frac{1212}{33}y^2 - \frac{793}{33}y - \frac{226}{33} > 0;$$

et comme $-\frac{1212}{33}$ est le plus grand coefficient négatif de cette inégalité, elle sera toujours satisfaite en faisant

$$y = \frac{1212}{33} + 1 = \frac{415}{11},$$

et à plus forte raison en faisant

$$y = \frac{415}{11} + u,$$

(u étant une quantité positive quelconque) d'où il résulte que la valeur de

$$x = \frac{11}{415 + 11u} < \frac{11}{415},$$

satisfaira à l'inégalité (58).

Maintenant l'on a

$$m = A z = (1 + x) z = \left(1 + \frac{11}{415 + 11u}\right) z = 6\left(\frac{426 + 11u}{415 + 11u}\right) q^3,$$

et partant

$$q^3 = \left(\frac{415 + 11u}{426 + 11u}\right) \frac{m}{6};$$

mais comme par hypothèse $q^3 < \frac{m}{6}$, il faudra trouver un nombre rationnel positif q, tel que q^3 soit compris entre

$$\frac{m}{6} \quad \text{et} \quad \frac{415\, m}{426 \times 6};$$

et il est clair qu'on pourra toujours trouver une infinité de valeurs de q^3 comprises entre ces limites, valeurs qui satisferont à toutes les *inégalités de condition* que nous venons de trouver.

Maintenant puisque le binome

$$\left(\frac{m + 6q^3}{6q^2}\right)^3 - \left(\frac{m}{6q^2}\right)^3,$$

se réduit à la somme de deux cubes positifs, à l'aide de l'identité (54), et que d'après l'analyse précédente on peut réduire l'autre binome

$$\left(\frac{m + 6q^3}{6q^2}\right)^3 \left(\frac{(m + 6q^3)^3 - 2m^3}{(m + 6q^3)^3 + m^3}\right)^3 - \left(\frac{m}{6q^2}\right)^3,$$

à la somme de deux cubes positifs à l'aide de l'équation (55), il est clair que l'on pourra réduire le second membre de l'équation

$$m = \left(\frac{m + 6q^3}{6q^2}\right)^3 + \left(\frac{m - 6q^3}{6q^2}\right)^3 - \left(\frac{m}{6q^2}\right)^3 - \left(\frac{m}{6q^2}\right)^3$$

à la somme de quatre cubes positifs; et partant on aura pour résultat, qu'un nombre quelconque rationnel positif peut toujours se décomposer, d'une infinité de manières, en quatre cubes positifs, en nombres rationnels.

Lagrange en cherchant les formes cubiques qui se reproduisent, lorsqu'elles sont multipliées entre elles, trouva la formule

$$(59)\ldots\left\{\begin{array}{l} x^3 + a x^2 y + (a^2 - 2b) x^2 z + b x y^2 + (ab - 3c) x y z \\ \quad + (b^2 - 2ac) x z^2 + c y^3 + a c y^2 z + b c y z^2 + c^2 z^3 \end{array}\right\},$$

qui étant multipliée par une formule semblable donne un produit de la même forme. D'après les principes que nous venons d'exposer on peut trouver un grand nombre d'expressions nouvelles, de la même espèce que la formule (59), et qui ne sont pas comprises dans celle-ci. En effet étant données les deux équations,

$$F = F_3(x\ ,\ y\ ,\ z\ ,\ u\ ,\ \ldots\ldots\ \text{etc.}) + A\ ,$$

$$F_1 = F_3(x_1\ ,\ y_1\ ,\ z_1\ ,\ u_1\ ,\ \ldots\ldots\ \text{etc.}) + A\ ,$$

on pourra toujours faire

$$F F_1 = F_3(r\ ,\ s\ ,\ t\ ,\ v\ ,\ \ldots\ldots\ \text{etc.}) + A\ ,$$

(les quantités r, s, t, v, ... etc., étant des fonctions rationnelles des quantités A, x, x_1, y, y_1, z, z_1, ... etc.) pourvu que l'équation

$$F_3(X\ ,\ Y\ ,\ Z\ ,\ U\ ,\ \ldots\ldots\ \text{etc.}) = 0\ ,$$

puisse être résolue en nombres rationnels. Ainsi par exemple en faisant

$$F = x^3 + y^3 + z^3 + u^3\ ,\quad F_1 = X^3 + Y^3 + Z^3 + U^3\ ,$$

on aura l'identité

$$FF_1 = \begin{cases} \left(\frac{FF_1+(r+s+t)^3-r^3-s^3-t^3}{3\left((r+s+t)^2+r^2-s^2-t^2\right)}-r-s-t\right)^3+\left(\frac{FF_1+(r+s+t)^3-r^3-s^3-t^3}{3\left((r+s+t)^2+r^2-s^2-t^2\right)}+r\right)^3 \\ \\ +\left(s-\frac{FF_1+(r+s+t)^3-r^3-s^3-t^3}{3\left((r+s+t)^2+r^2-s^2-t^2\right)}\right)^3+\left(t-\frac{FF_1+(r+s+t)^3-r^3-s^3-t^3}{3\left((r+s+t)^2+r^2-s^2-t^2\right)}\right)^3 \end{cases}$$

dans laquelle r, s, t, sont des quantités indéterminées.

Euler a démontré pour la première fois, qu'un nombre quelconque rationnel positif est toujours égal à la somme de quatre carrés en nombres rationnels; il a démontré aussi, que le produit d'une somme de quatre carrés, par une somme de quatre carrés, est semblablement la somme de quatre carrés: l'analyse précédente montre que l'on peut généraliser ces deux théorèmes, et les étendre aux troisièmes puissances.

La méthode que nous avons exposée n'est plus générale, lorsque les formules que l'on considère passent le troisième degré; et c'est à ce degré qu'Euler et Lagrange se sont arrêtés dans leurs recherches. Cependant on peut trouver des formules de tous les degrés qui se reproduisent lorsqu'elles sont multipliées par des formules semblables. Ainsi, par exemple, pour le quatrième degré on a les deux formules

$$3\,x^4 + y^4 - z^4 - 3\,u^2 \quad ,$$

$$30\,x^4 + 2\,y^4 - 20\,z^4 - 12\,u^3 \quad ,$$

qui représentent rationnellement tous les nombres rationnels, et chacune desquelles se reproduit lorsqu'elle est multipliée par une formule semblable.

Lagrange en partant de la formule (59) a trouvé une infinité de solutions entières de l'équation

$$F_3(x\,,y) = ax^3 + bx^2y + cxy^2 + dy^3 = z^2 \;;$$

et il a cru que cette équation offrirait beaucoup de difficultés si on voulait la résoudre autrement que par sa méthode: nous allons voir maintenant qu'elle est un cas particulier d'une équation générale dont on peut toujours avoir une infinité de solutions entières.

Soit proposé de résoudre en nombres entiers l'équation

$$(60)\ldots\left\{\begin{array}{l}\mathrm{F}_n(x_1, y_1, z_1, \ldots \text{etc.}) + \mathrm{F}_m(x_2, y_2, z_2, \ldots \text{etc.}) \\ \quad \ldots\ldots\ldots\ldots\ldots + \mathrm{F}_p(x_r, y_r, z_r, \ldots \text{etc.})\end{array}\right\} = \mathrm{F}_q(x_s, y_s, z_s \ldots \text{etc.}),$$

dans laquelle on exprime toujours en général par

$$\mathrm{F}_p(x_r\ ,\ y_r\ ,\ z_r\ ,\ \ldots\ldots \text{etc.})\ ,$$

un polynome homogène, rationnel et entier, du degré p (p étant un nombre entier positif) à coefficiens entiers entre les variables

$$x_r\ ,\ y_r\ ,\ z_r\ ,\ \ldots\ldots \text{etc.}\ ;$$

si l'un quelconque des exposans n , m , ... p , q , n'a de facteur commun avec aucun des autres exposans, on pourra toujours résoudre d'une infinité de manières l'équation (60). En effet, soit q l'exposant qui n'a de facteur commun avec aucun des autres exposans n , m , ... p ; on mettra u à la place des inconnues x_s , y_s , z_s , ... etc. dans le polynome

$$\mathrm{F}_q(x_s\ ,\ y_s\ ,\ z_s\ ,\ \ldots\ldots \text{etc.})\ ,$$

et en supposant que la somme des coefficiens du polynome

$$\mathrm{F}_q(x_s\ ,\ y_s\ ,\ z_s\ ,\ \ldots\ldots \text{etc.})\ ,$$

soit égale à b , on aura

$$\mathrm{F}_q(u\ ,\ u\ ,\ u\ ,\ \ldots\ldots \text{etc.}) = b\,u^q\ ;$$

puis en faisant, pour abréger, le nombre a égal au produit $n \times m \times \ldots \times p$, on écrira dans l'équation (60) , $(bX)^{\frac{a}{n}}$ à la place de x , $(bY)^{\frac{a}{n}}$ à la place de y , $(bZ)^{\frac{a}{n}}$ à la place de z , ... etc.; puis on écrira $(bX_1)^{\frac{a}{m}}$, à la place

de x_1, $(bY_1)^{\frac{a}{m}}$ à la place de y_1, $(bZ_1)^{\frac{a}{m}}$ à place de z_1, ... etc.; et ainsi de suite jusqu'au dernier polynome du premier membre dans laquel on écrira $(bX_r)^{\frac{a}{p}}$ à la place de x_r, $(bY_r)^{\frac{a}{p}}$ à la place de y_r, $(bZ_r)^{\frac{a}{p}}$ à la place de z_r, ... etc.; où il faut observer que les quantités

$$\begin{array}{l} X \;,\; Y \;,\; Z \;,\; \ldots\ldots\ldots \text{ etc.} \;, \\ X_1 \;,\; Y_1 \;,\; Z_1 \;,\; \ldots\ldots\ldots \text{ etc.} \;, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_r \;,\; Y_r \;,\; Z_r \;,\; \ldots\ldots\ldots \text{ etc.} \;, \end{array}$$

expriment des nombres entiers quelconques.

Maintenant pour déterminer la valeur de u, l'on faira

$$\left\{\begin{array}{l} \frac{1}{b}\,\mathrm{F}_n\left((bX)^{\frac{a}{n}},\ (bY)^{\frac{a}{n}},\ (bZ)^{\frac{a}{n}},\ldots\ldots \text{etc.}\right) \\ +\frac{1}{b}\,\mathrm{F}_m\left((bX_1)^{\frac{a}{m}},\ (bY_1)^{\frac{a}{m}},\ (bZ_1)^{\frac{a}{m}},\ldots\ldots \text{etc.}\right) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ +\frac{1}{b}\,\mathrm{F}_p\left((bX_r)^{\frac{a}{p}},(bY_r)^{\frac{a}{p}},\ (bZ_r)^{\frac{a}{p}},\ldots\ldots \text{etc.}\right) \end{array}\right\} = u \,,$$

et il clair que u sera un nombre entier. A présent si l'on multiplie tous les termes de cette équation par u^{at}, (t étant l'un des nombres entiers et positifs qui résolvent l'équation à deux inconnues $at + 1 = qv$) et que dans l'équation (60) l'on fasse

$$x = (b X u^t)^{\frac{a}{n}},\ y = (b Y u^t)^{\frac{a}{n}},\ z = (b Z u^t)^{\frac{a}{n}}, \ldots \text{etc.},$$

$$x_1 = (b X_1 u^t)^{\frac{a}{m}},\ y_1 = (b Y_1 u^t)^{\frac{a}{m}},\ z_1 = (b Z_1 u^t)^{\frac{a}{m}}, \ldots \text{etc.},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$x_r = (b X_r u^t)^{\frac{a}{p}},\ y_r = (b Y_r u^t)^{\frac{a}{p}},\ z_r = (b Z_r u^t)^{\frac{a}{p}}, \ldots \text{etc.},$$

on aura résolu l'équation proposée d'une infinité de manières, et l'on obtiendra l'identité

$$\left\{\begin{array}{l} F_n\left((b X u^t)^{\frac{a}{n}}, (b Y u^t)^{\frac{a}{n}}, (b Z u^t)^{\frac{a}{n}}, \ldots\ldots \text{etc.}\right) \\ + F_m\left((b X_1 u^t)^{\frac{a}{m}}, (b Y_1 u^t)^{\frac{a}{m}}, (b Z_1 u^t)^{\frac{a}{m}}, \ldots\ldots \text{etc.}\right) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ + F_p\left((b X_r u^t)^{\frac{a}{p}}, (b Y_r u^t)^{\frac{a}{p}}, (b Z_r u^t)^{\frac{a}{p}}, \ldots\ldots \text{etc.}\right) \end{array}\right\} = F_q(u^v, u^v, u^v, \ldots \text{etc.}).$$

Il serait facile de généraliser cette méthode, et de l'appliquer à beaucoup d'autres équations composées de polynomes qui seraient toujours homogénes, mais qui pourraient être fractionnaires et même transcendans; néanmoins comme ces recherches ne présentent aucune difficulté, nous croyons ne pas devoir nous y arrêter plus long tems.

Ce mémoire faisait partie d'un travail sur la théorie des nombres présenté en 1823 à l'Académie Royale des Sciences de Paris.

MÉMOIRE

SUR LA

RÉSOLUTION DES ÉQUATIONS INDÉTERMINÉES

À L'AIDE DES SÉRIES.

INTRODUCTION.

Les formules qui servent à résoudre en termes finis les problèmes analytiques sont si peu nombreuses, qu'il n'y aurait que des questions très-simples que l'on pourrait traiter sans le calcul des séries. Cependant jusqu'à présent on n'avait jamais tenté d'appliquer ce calcul aux équations indéterminées, que l'on tâchait de résoudre par des transformations, en s'aidant des propriétés spéciales des nombres, que le génie de quelques grands géomètres avait pu découvrir; quoique dans le seul cas de l'analyse indéterminée, les méthodes d'approximation fournissent des solutions exactes. Car comme, lorsqu'il s'agit d'équations indéterminées, les inconnues doivent avoir des valeurs entières, il est clair qu'ayant trouvé deux limites entre lesquelles doit être comprise la valeur d'une inconnue, cette valeur ne peut être que l'un des nombres entiers compris entre ces deux limites. D'où il résulte qu'en égalant successivement à tous ces nombres entiers l'inconnue dont il s'agit, on pourra, par l'élimination, ôter cette inconnue de l'équation proposée, qui se réduira de cette manière à un système d'équations dans lesquelles le nombre des inconnues sera diminué de l'unité.

Dans ce mémoire nous appliquons le calcul des séries aux équations indéterminées. Notre méthode est fondée sur ce théorème très-simple, que lorsqu'on a une équation dont chaque membre se compose de deux termes, l'un desquels est un nombre entier, et l'autre est une fraction moindre que l'unité, il faudra que les deux nombres entiers soient égaux entre eux, de même que les deux fractions. Il résulte de là que lorsque d'une équation indéterminée à deux inconnues, on aura déduit la valeur d'une fonction donnée des inconnues

développée en série convergente, de manière qu'une partie de la série soit une fonction entière des inconnues, et l'autre partie soit une fonction fractionnaire telle qu'on puisse la rendre plus petite que l'unité, en donnant aux inconnues une valeur plus grande que des limites données, il faudra que ces inconnues soient comprises entre ces limites, ou bien on pourra égaler à zéro la partie fractionnaire, et la partie entière de la série fournira de cette manière une nouvelle équation à deux inconnues qui devra exister en même tems que l'équation proposée, et qui servira à résoudre celle-ci complètement.

Nous appliquons d'abord ces principes à des équations indéterminées très-simples, en montrant comment, par le développement en séries, on peut les décomposer en deux autres équations, dont l'une en termes finis ne renferme que des quantités entières. Puis nous résolvons des équations plus compliquées algébriques ou transcendantes. Nous montrons ensuite comment l'on peut résoudre les équations dans lesquelles il faut extraire les racines, d'un ordre quelconque, de certains polynomes donnés, et nous faisons voir que dans ce cas, afin que notre méthode soit applicable, il faut satisfaire à la condition que l'on puisse extraire la racine de l'ordre dont il s'agit, du terme qui contient le plus grand exposant. Enfin nous résolvons l'équation proposée par rapport à l'une des inconnues, lorsque cette résolution est possible, en faisant observer que dans ce cas, lorsque, en donnant aux inconnues ou à l'une d'elles seulement des valeurs plus grandes qu'un nombre donné, les racines deviennent imaginaires, il faudra nécessairement prendre pour les inconnues des valeurs moindres que ce nombre, et l'équation proposée sera résolue complètement.

En traitant de cette manière les équations indéterminées qui sont du second degré par rapport à l'une des inconnues, nous montrons quelles sont les conditions auxquelles on doit satisfaire afin de pouvoir résoudre complètement ces équations. Nous trouvons aussi les conditions auxquelles doivent satisfaire les équations qui sont du troisième degré par rapport à l'une des inconnues, afin qu'on puisse les résoudre complètement à l'aide des formules qui donnent les racines des équations du troisième degré. On pourrait faire les mêmes considérations sur les équations qui sont du quatrième degré par rapport a l'une des inconnues, quoique dans ce cas ces recherches se compliquent beaucoup. Mais comme passé le quatrième degré on n'a aucune méthode par trouver les racines des équations algébriques, nous ne pourrions pas aller plus loin par des formules finies, et nous avons dû recourir aux méthodes d'approximation.

Si l'on cherche, par le théorème de Lagrange, l'expression en séries des racines d'une équations algébrique quelconque, ou obtient plusieurs développemens, parmi lesquels il faut choisir ceux qui deviennent convergens lorsqu'on y substitue les valeurs des coefficiens. En général ces développemens contiennent des radicaux, mais quelquefois ils en sont délivrés, selon le degré de l'équation proposée et le nombre des termes qu'elle renferme. Maintenant, si l'on suppose qu'il s'agisse de résoudre une équation indéterminée à deux inconnues, il est clair que l'on pourra la résoudre, par le théoréme de Lagrange, par rapport à l'une des inconnues, en considérant les coefficieus comme des fouctions de l'autre inconnue. Alors lorsque la série sera convergente, et que l'on pourra faire disparaître les irrationnels qu'elle contiendra, on obtiendra une équation composée d'une partie entière et d'une partie fractionnaire; et si l'on rend celle-ci plus petite que l'unité (en donnant à l'inconnue qu'elle renferme une valeur plus grande qu'une limite donnée) on aura une nouvelle équation qui devra subsister en même tems que l'équation proposée, ou bien il faudra donner à l'une des inconnues une valeur moindre que la limite dont on vient de parler; et dans les deux cas l'équation proposée sera résolue complètement.

En traitant de cette manière les équations qui sont du second ou du troisième degré par rapport à l'une des inconnnes, nous retrouvons les conditions que nous avons déjà obtenues en considérant la forme des racines; et même nous trouvons de nouveaux cas de solution. Enfiu nous montrons de quelle manière on peut résoudre les équations plus générales, et nous exposons quelques artifices analytiques qui peuvent servir à la résolution de plusieurs équations indéterminées.

Lorsque la série dout on doit faire usage pour avoir la valeur de la racine cherchée contient des quantités irrationnelles, notre méthode exige pour être applicable, que l'on puisse résoudre une nouvelle équation indéterminée avant d'obtenir la résolution de l'équation proposée: mais lorsque l'irrationnalité ne se moutre pas, il suffira d'obtenir une série convergente qui fournira la résolution complète du problème; et il faut remarquer que les conditions qui doivent être satisfaites dans tous les cas, afin de résoudre par cette méthode les équations indéterminées à deux inconnues, ne regardent que les termes qui dans chaque coefficient de l'inconnue, par rapport à laquelle on a résolu l'équation, renferment les plus grandes puissances de la variable.

En général au lieu de chercher le développement en séries d'une racine de

l'équation proposée, on pourra chercher une fonction quelconque des inconnues, et si la suite que l'on obtient de cette manière peut devenir convergente, on aura résolu complètement l'équation proposée.

La méthode que nous exposons dans ce mémoire sert à trouver la résolution d'une infinité d'équations indéterminées de tous les degrés, que l'on ne saurait résoudre d'aucune manière par les principes connus. On peut aussi l'appliquer aux équations contenant un plus grand nombre d'inconnues, en les résolvant successivement par rapport à toutes les inconnues l'une après l'autre.

ANALYSE.

Etant donnée l'équation

$$(61) \ldots\ldots\ldots\ldots A + \alpha = B + \beta ,$$

dans laquelle A et B sont deux nombres entiers, et α et β sont deux quantités quelconques plus petites que l'unité, il est clair que l'on aura

$$A = B , \quad \alpha = \beta .$$

Il résulte de là que si d'une équation à deux inconnues $\varphi(x , y) = 0$, on peut tirer, d'une manière quelconque, une équation de la forme (61), on pourra déterminer, par l'élimination entre les deux équations

$$\varphi(x , y) = 0 , \quad A = B ,$$

les valeurs de x et de y. En général étant proposé de résoudre en nombres entiers l'équation à n inconnues

$$\varphi(x , y , z , \ldots\ldots \text{etc.}) = 0 ,$$

si l'on en peut déduire, par des opérations quelconques, le m équations

$$A_1 + \alpha_1 = B_1 + \beta_1 ; \; A_2 + \alpha_2 = B_2 + \beta_2 , \ldots A_m + \alpha_m = B_m + \beta_m ,$$

dans lesquelles les quantités

$$A_1 \ , \ A_2 \ , \ldots\ldots A_m \ , \ B_1 \ , \ B_2 \ , \ldots\ldots B_m \ ,$$

sont des nombres entiers, et les quantités

$$\alpha_1 \ , \ \alpha_2 \ , \ldots\ldots \alpha_m \ , \ \beta_1 \ , \ \beta_2 \ , \ldots\ldots \beta_m \ ,$$

sont des fractions plus petites que l'unité, on trouvera les équations

$$A_1 = B_1 \ , \ A_2 = B_2 \ , \ldots\ldots A_m = B_m \ ,$$

qui étant combinées avec l'équation

$$\varphi(x \ , \ y \ , \ z \ , \ \ldots\ldots \text{etc.}) = 0 \ ,$$

donneront, après l'élimination, une équation qui ne contiendra plus que $n - m$ inconnues.

Nous répèterons ici la remarque que nous avons déjà faite précédemment, que si par un procédé quelconque, on est parvenu à tirer de l'équation

$$\varphi(x \ , \ y \ , \ z \ , \ \ldots\ldots \text{etc.}) = 0 \ ,$$

une valeur approchée δ de x telle, que l'on sache seulement que la valeur de δ doit être toujours comprise entre M et N, on trouvera la valeur exacte de x en l'égalant successivement à tous les nombres entiers compris entre M et N.

Maintenant soit proposé de résoudre en nombres entiers l'équation

$$y = \frac{a + a_1 x + a_2 x^2 \ldots\ldots + a_n x^n}{b + b_1 x + b_2 x^2 \ldots\ldots + b_m x^m} \ ;$$

on faira d'abord

$$a + a_1 x \ldots\ldots + a_n x^n = \mathrm{X}_n \ , \quad b + b_1 x \ldots\ldots + b_m x^m = \mathrm{X}_m \ ,$$

et en général X_r représentera un polynome en x du degré r à coefficiens

rationnels : par conséquent il s'agira de résoudre en nombres entiers l'équation

$$y = \frac{X_n}{X_m}$$

dans laquelle nous distinguerons trois cas différens, selon que l'on aura

$$m > n \quad , \quad m = n \quad , \quad m < n \quad .$$

Soit $m > n$; on pourra déterminer facilement un nombre entier L tel qu'en substituant pour x dans la fraction $\frac{X_n}{X_m}$ la valeur $L + \alpha$ (α étant une quantité quelconque réelle et positive) on ait toujours (abstraction faite des signes) $X_m > X_n$; on pourra de même déterminer une seconde limite inférieure L_1 telle que si l'on fait $x = L_1 - \alpha$ on ait encore $X_m > X_n$; et comme si l'équation proposée est résoluble il faudra que la fraction $\frac{X_n}{X_m}$ soit un nombre entier, on ne pourra donner à x que les valeurs suivantes

$$x = L_1 \ , \ x = L_1 + 1 \ , \ \ldots\ldots \ x = L \ ;$$

de sorte qu'en éliminant x successivement entre l'équation proposée et l'une des équations précédentes, on aura un nombre $L + 1 - L_1$ d'équations en y, dont les racines entières, s'il en existe, fourniront toutes les solutions de l'équation proposée.

Lorsque $m = n$, on divisera X_n par X_m et on obtiendra un quotient $\frac{a_m}{b_m}$ plus un reste qui sera de la forme $\frac{X_{m-1}}{X_m}$, en indiquant toujours par X_{m-1} un polynome en x du degré $m - 1$ à coefficiens rationnels. Maintenant on aura, lorsque $n = m$,

$$y = \frac{X_n}{X_m} = \frac{a_m}{b_m} + \frac{X_{m-1}}{X_m} \ ,$$

et partant

$$b_m\, y = a_m + b_m \frac{X_{m-1}}{X_m} \ ,$$

d'où il résulte qu'en faisant $b_m y - a_m = z$, on devra résoudre en nombres entiers l'équation

$$z = b_n \frac{X_{m-1}}{X_m}$$

dont nous savons déjà trouver toutes les solutions entières.

Lorsque $n > m$, on faira $n = m + p$, et en effectuant la division on trouvera l'équation

$$y = \frac{X_n}{X_m} = A\, x^p + A_1\, x^{p-1} \ldots\ldots + A_p + \frac{X_{m-1}}{X_m} \quad ,$$

dans laquelle les coefficiens A, A_1, ... A_p, sont des nombres rationnels, et X_{m-1} est un polyuome en x du degré $m - 1$ à coefficiens rationnels. A présent si l'on réduit tous les coefficiens de cette équation au dénominateur commun D, on aura

$$D\, y = D\,(A\, x^p + A_1\, a^{p-1} \ldots\ldots + A_p) + \frac{D\, X_{m-1}}{X_m} \quad ,$$

et par conséquent

$$D\, y - D\,(A x^p + A_1\, x^{p-1} \ldots\ldots + A_p) = \frac{D\, X_{m-1}}{X_m} \quad ,$$

et comme le premier membre de cette équation est un nombre entier, si on l'égale à z, on devra résoudre l'équation

$$z = \frac{X_{m-1}}{X_m} \quad ,$$

dont nous savons déjà trouver toutes les solution entières.

A l'aide de l'équation

$$y = \frac{a + a_1\, x + a_2\, x^2 \ldots\ldots + a_n\, x^n}{b + b_1\, x + b_2\, x^2 \ldots\ldots + b_m\, x^m} = \frac{X_n}{X_m} \; ,$$

on peut résoudre l'autre plus générale

$$\varphi(x\,,\,y) = \frac{X_n}{X_m}\quad,$$

en indiquant par $\varphi(x\,,y)$ une fonction rationnelle et entière des nombres entiers x et y ; car puisque le premier membre de cette équation est un nombre entier, on pourra trouver toutes les valeurs de x qui rendent entier le second membre, et comme le nombre des valeurs entières que peut prendre le second membre est toujours limité, si on les représente par v_1 , v_2 , ... v_r , on aura les équations

$$\varphi(x\,,y) = v_1\quad,\quad \varphi(x\,,y) = v_2\quad,\quad \ldots\ldots \varphi(x\,,y) = v_r\quad,$$

qui devront exister en même tems que l'équation

$$\varphi(x\,,\,y) = \frac{X_n}{X_m}\quad,$$

et qui serviront, par l'élimination, à trouver toutes les solutions de celle-ci.

L'équation que nous venons de traiter en renferme un grand nombre d'autres plus générales. Ainsi par esemple étant proposé de résoudre en nombres entiers l'équation

$$F(x)\,.\,F_1(y) \;=\; f(x)\,.\,f_1(y)\quad,$$

dans laquelle F , F_1 , f , f_1 , expriment des fonctions entières et rationnelles, on faira d'abord

$$F(x) = X_n\quad,\quad f(x) = X_m\quad,\quad F_1(y) = Y_p\quad,\quad f_1(y) = Y_q\quad,$$

en exprimant toujours par X_n et X_m des polynomes en x , entiers et rationnels des degrés n et m , et par Y_p et Y_q des polynomes en y , entiers et rationnels des degrés p et q , et l'on aura

$$\frac{F(x)}{f(x)} = \frac{X_n}{X_m} = \frac{f_1(y)}{F_1(y)} = \frac{Y_q}{Y_p}\;;$$

d'où l'on déduira une équation de la forme

$$X_{n-m} + \frac{X_{m-1}}{X_m} = Y_{q-p} + \frac{Y_{p-1}}{Y_p} ,$$

et par conséquent on pourra trouver pour x et y, des limites telles, qu'en prenant pour ces inconnues des valeurs hors de ces limites, on ait toujours, après avoir réduit tous les coefficiens fractionnaires au même dénominateur D, l'équation

$$D\,X_{n-m} = D\,Y_{p-q} ,$$

qui étant combinée avec l'équation proposée fournira toutes les valeurs des inconnues, qui ne sont pas comprises entre les limites dont on vient de parler; et comme les valeurs comprises entre ces limites peuvent se déterminer séparément avec facilité, on aura toutes les solutions entières de l'équation proposée. Dans l'analyse précédente nous avons supposé $n > m$, mais si l'on avait $n = m$, ou $n < m$, on renverserait la fraction, et l'on aurait

$$\frac{X_m}{X_n} = \frac{Y_p}{Y_q} ;$$

et en général il serait facile de résoudre cette équation dans tous les cas.

Soient X_n, X_m, X_r, X_p, des polynomes quelconques en x entiers, des degrés n, m, r, p, et supposons que l'on ait $p > r$, $n > m$; si l'on doit trouver toutes les solutions entières de l'équation

$$(62)\ldots y = \frac{X_n}{X_m}\left(A + A_1\frac{X_r}{X_p} + A_2\left(\frac{X_r}{X_p}\right)^2 \ldots + A_{t-1}\left(\frac{X_r}{X_p}\right)^{t-1} + A_t\left(\frac{X_r}{X_p}\right)^t + \text{etc.}\right),$$

dans laquelle la valeur du rapport $\frac{A_t}{A_{t-1}}$ ne peut jamais surpasser une limite L, on poussera la série jusqu'au terme $t + 1.^{\text{me}}$, (en prenant pour t le plus petit nombre entier qui satisfait à l'inégalité $pt + m > rt + n$, laquelle sera toujours possible puisque $p > r$) et on aura, après avoir effectué les divisions et après avoir multiplié par le dénominateur commun D, une équation de la forme

$$D\,y = a\,x^{n-m} + a_1\,x^{n-m-1} \ldots\ldots + a_{n-m} + \frac{f(x)}{f_1(x)} ,$$

dans laquelle la fraction $\frac{f(x)}{f_1(x)}$ représente une série convergente, dont la valeur pourra se réduire aussi petite que l'on voudra, en donnant à x des valeurs qui ne soient pas comprises entre deux limites l, l_1, que l'on déterminera aisément. On voit par là que l'équation proposée sera résolue complètement, par les principes que nous avons exposés précédemment, quelle que soit la nature de la fonction, algébrique ou transcendante, qui est exprimée par le second membre de l'équation (62).

Soit proposé maintenant de résoudre en nombres entiers l'équation

$$(63) \dots A a^n x^{pn} + b x^{pn-1} \dots + d x + c = A q^n y^{mn} + b_1 y^{mn-1} \dots + d_1 y + e_1 \; ,$$

on pourra d'abord multiplier tous ses termes par A^{n-1}, et en faisant ensuite

$$A^{n-1}(b x^{m-1} \dots\dots + d x + e) = r \; , \; A^{n-1}(b_1 y^{mn-1} \dots\dots + d_1 y + e) = s \; ,$$

on aura

$$A a \; x^p \sqrt[n]{1 + \frac{r}{A^n a^n x^{pn}}} = A q \; y^n \sqrt[n]{1 + \frac{s}{A^n q^m y^{mn}}} \; ,$$

et partant

$$A a \, x^p \left(1 + \frac{r}{n A^n a^n x^{pn}} - \text{etc.}\right) = A q \, y^m \left(1 + \frac{s}{n A^n q^n y^{mn}} - \text{etc.}\right) ,$$

et cette équation étant traitée de la même manière que l'équation (62) nous conduira nécessairement à la résolution de l'équation proposée, puisque les séries qu'elles contient sont toujours convergentes, lorsqu'on donne à x et y des valeurs plus grandes que des quantités données.

Si l'on exprime en géneral (comme on l'a déjà fait dans le mémoire précédent) par $F_r(x, y)$, un polynome homogène et entier en x et y, du degré r, on pourra résoudre aussi l'équation

$$a^n y^{mn} = b^n x^{pn} + F_{n-1}(x, y) + F_{n-2}(x, y) \dots\dots + c = b^n x^{pn} + f(x, y) \; ;$$

car en extrayant la racine n.^{me} on aura



$$ay^m = bx^p \sqrt[n]{1 + \frac{f(x, y)}{b^n x^{pn}}} = bx^p \left(1 + \frac{f(x, y)}{n b^n x^{pn}} - \text{etc.}\right),$$

ou bien

$$bx^p = ay^m \sqrt[p]{1 + \frac{f(x, y)}{a^n y^{mn}}} = ay^m \left(1 + \frac{f(x, y)}{n a^n y^{mn}} - \text{etc.}\right),$$

et il faudra faire usage de la première ou de la seconde série, selon que l'on aura $x > y$, ou $y > x$; et dans les deux cas on pourra déterminer deux limites de x et y, telles qu'en prenant pour ces inconnues des nombres entiers hors de ces limites, on ait l'équation

$$F(x, y) = F_1(x, y),$$

qui devra exister en même que l'équation proposée, dont on pourra, de cette maniere, trouver toutes les solutions entières.

On peut résoudre par les mêmes principes l'équation

$$y = \frac{X_p}{\sqrt[n]{(a^n x^{mn} + b x^{mn-1} \ldots\ldots + c)}},$$

qui donnera

$$y = \frac{X_p}{a x^m + a_1 x^{m-1} \ldots\ldots + a_m + \frac{a_{m+1}}{x} + \text{etc.}},$$

d'où l'on déduira une équation de la forme

$$Dy = X_{p-m} + \frac{X_{m-1}}{X_m},$$

qui servira à trouver toutes les solutions entières de l'équation proposée. L'équation

$$y = \frac{X_p}{\sqrt[n]{(a^n x^{mn} + b x^{mn-1} \ldots\ldots + c)}}$$

peut se résoudre aussi en observant que l'on a

$$y^n = \frac{(X_p)^n}{a^n x^{mn} + b x^{mn-1} \ldots\ldots + c},$$

et il est clair que l'on pourra résoudre de la même manière les équations de la forme

$$y = \frac{X_p}{\sqrt[r]{X_{ar}}}\left(A + A_1 \frac{X_s}{X_t} + A_2 \left(\frac{X_s}{X_t}\right)^2 + \text{etc.} \right),$$

pourvu que l'on ait $s > t$, et que le rapport de deux coefficiens consécutifs quelconques, de la série comprise dans le second membre, ne puisse jamais devenir infini.

L'équation (63) renferme la suivante

$$A^2 x^2 = a^2 y^{2m} + b y^{2m-1} \ldots\ldots + py + q,$$

qui sert à trouver la résolution complète, en nombres entiers, de l'équation

$$(64) \ldots x^2(ay^n + by^{n-1} \ldots + cy + d) + x(ey^r + fy^{r-1} \ldots + gy + h) + iy^m + ky^{m-1} \ldots + l = 0,$$

lorsque $2r > n + m$, et lorsque $2r$ étant moindre que $n + m$ on peut faire en nombres entiers $-ai\,y^{m+n} = p^2 y^{2s}$. En effet, en résolvant l'équation (64) par rapport à x, on trouve

$$2x(ay^n + by^{n-1} \ldots\ldots + cy + d) + ey^r + fy^{r-1} \ldots\ldots + gy + h =$$

$$\sqrt{\left((ey^r + fy^{r-1} \ldots + gy + h)^2 - 4(ay^n + by^{n-1} \ldots + cy + d)(iy^m + ky^{m-1} \ldots + l)\right)},$$

et puisque le premier membre de cette équation est un nombre entier, le second devra l'être aussi, et il faudra résoudre en nombres entiers l'équation

$$(ey^r + fy^{r-1} \ldots + gy + h)^2 - (4ay^n + by^{n-1} \ldots + cy + d)(iy^m + ky^{m-1} \ldots + l) = z^2,$$

ce qu'on pourra toujours faire par notre méthode lorsque on aura $2r > n + m$,

et lorsque on aura $2r < n + m$ et $-iay^{n+m} = p^2 y^{2s}$. Il faut observer ici que puisque de l'équation

$$Ax^2 + Bx + C = 0,$$

on déduit

$$2Ax + B = \pm \sqrt{B^2 - 4AC},$$

la résolution de l'équation (64) dérive, dans le cas de $2r > n + m$, de la forme des racines des équations du second degré qui admettent sous le radical le coefficient B élevé au carré, sans qu'il soit nécessaire de satisfaire à aucune autre condition; tandis que dans l'autre cas il faut satisfaire en nombres entiers aux équations $-ia = p^2$, $m + n = 2s$. Lorsque $2r < n + m$, et que le produit ia est positif, on pourra toujours avoir toutes les solutions positives de l'équation (64); tandis que si le produit ia est négatif, on pourra avoir toutes les solutions négatives de la même équation. Mais si l'on a $2r < n + m$, $m + n = 2s$, et que le produit ai soit positif, on pourra résoudre complètement l'équation (64). Et l'on voit que toutes les conditions précédentes ne regardent que les termes qui, dans les coefficiens des diverses puissances de x comprises dans l'équation (64), contiennent les plus grandes puisances de y.

Soit proposé maintenant de résoudre en nombres entiers l'équation du troisième degré à deux inconnues

$$(65) \ldots\ldots \quad Y_r x^3 + Y_n x + Y_m = 0,$$

dans laquelle on a

$$Y_r = ay^r + a_1 y^{r-1} \ldots\ldots + a_r,$$

$$Y_n = by^n + b_1 y^{n-1} \ldots\ldots + b_n,$$

$$Y_m = cy^m + c_1 y^{m-1} \ldots\ldots + c_m,$$

si l'on cherche les trois racines de l'équation (65), on aura par les formules

connues

$$x = \sqrt[3]{\left(-\frac{Y_m}{2Y_r} + \sqrt{\left(\frac{(Y_m)^2}{4(Y_r)^2} + \frac{(Y_n)^3}{27(Y_r)^3}\right)}\right)} + \sqrt[3]{\left(-\frac{Y_m}{2Y_r} - \sqrt{\left(\frac{(Y_m)^2}{4(Y_r)^2} + \frac{(Y_n)^3}{27(Y_r)^3}\right)}\right)} ,$$

$$x = \sqrt[3]{\left(-\frac{Y_m}{2Y_r} + \sqrt{\left(\frac{(Y_m)^2}{4(Y_r)^2} + \frac{(Y_n)^3}{27(Y_r)^3}\right)}\right)}\left(\frac{-1+\sqrt{-3}}{2}\right) + \sqrt[3]{\left(-\frac{Y_m}{2Y_r} - \sqrt{\left(\frac{(Y_m)^2}{4(Y_r)^2} + \frac{(Y_n)^3}{27(Y_r)^3}\right)}\right)}\left(\frac{-1-\sqrt{-3}}{2}\right) ,$$

$$x = \sqrt[3]{\left(-\frac{Y_m}{2Y_r} + \sqrt{\left(\frac{(Y_m)^2}{4(Y_r)^2} + \frac{(Y_n)^3}{27(Y_r)^3}\right)}\right)}\left(\frac{-1-\sqrt{-3}}{2}\right) + \sqrt[3]{\left(-\frac{Y_m}{2Y_r} - \sqrt{\left(\frac{(Y_m)^2}{4(Y_r)^2} + \frac{(Y_n)^3}{27(Y_r)^3}\right)}\right)}\left(\frac{-1+\sqrt{-3}}{2}\right) ,$$

et si l'on suppose que l'on ait (abstraction faite des signes)

$$\frac{(Y_m)^2}{4(Y_r)^2} > \frac{(Y_n)^3}{27(Y_r)^3} ,$$

on pourra développer en série le radical

$$\sqrt{\left(\frac{(Y_m)^2}{4(Y_r)^2} + \frac{(Y_n)^3}{27(Y_r)^3}\right)} ,$$

par les puissances ascendantes de $\frac{Y_n}{3Y_r}$, et l'on obtiendra la série convergente

$$\frac{Y_m}{2Y_r} + \left(\frac{(Y_n)^3}{2 . 27 (Y_r)^3}\right)\left(\frac{2Y_r}{Y_m}\right) \ldots\ldots + \text{etc.} ,$$

qui, étant substituée dans la formule

$$\sqrt[3]{\left(-\frac{Y_m}{2Y_r} + \sqrt{\left(\frac{(Y_m)^2}{4(Y_r)^2} + \frac{(Y_m)^3}{27(Y_r)^3}\right)}\right)} ,$$

donnera

$$\sqrt[3]{\left(-\frac{Y_m}{2\,Y_r}+\frac{Y_m}{2\,Y_r}+\left(\frac{(Y_n)^3}{27\,(Y_r)^3}\right)\left(\frac{Y_r}{Y_m}\right)+\text{etc.}\right)}=\sqrt[3]{\left(\left(\frac{(Y_n)^3}{27\,(Y_r)^3}\right)\left(\frac{Y_r}{Y_m}\right)+\text{etc.}\right)}$$

et l'on voit que si l'on peut satisfaire à l'équations $\frac{a}{b} = u^3$, en nombres rationnels, et à l'équation $r - m = 3s$ en nombres entiers, on pourra extraire la racine cubique de la quantité $\frac{Y_r}{Y_m}$; de même si l'on substitue la valeur du radical

$$\sqrt{\left(\frac{(Y_m)^2}{4\,(Y_r)^2} + \frac{(Y_n)^3}{27\,(Y_r)^3}\right)},$$

dans la formule

$$\sqrt[3]{\left(-\frac{Y_m}{2\,Y_r}-\sqrt{\left(\frac{(Y_m)^2}{4\,(Y_r)^2}+\frac{(Y_n)^3}{27\,(Y_r)^3}\right)}\right)},$$

on trouvera

$$\sqrt[3]{\left(-\frac{Y_m}{2\,Y_r}-\frac{Y_m}{2\,Y_r}-\left(\frac{(Y_n)^3}{27\,(Y_r)^3}\right)\left(\frac{Y_r}{Y_m}\right)-\text{etc.}\right)}$$

$$=\sqrt[3]{\left(-\frac{Y_m}{Y_r}-\text{etc.}\right)},$$

et si l'on pourra faire

$$\frac{Y_m}{Y_r} = A^3 y^{3t} + B y^{3t-1} + \text{etc.},$$

il est clair que l'on pourra extraire la racine cubique de la quantité

$$\sqrt[3]{\left(-\frac{Y_m}{Y_r}+\text{etc.}\right)},$$

et l'on voit que l'on trouvera les mêmes conditions que nous avons déjà obtenues, c'est à dire l'équation $\frac{a}{c} = u^3$, qui devra être résoluble en nombres rationnels, et l'équation $r - m = 3s$ que l'on devra résoudre en nombres entiers.

Il résulte de l'analyse précédente, que lorsqu'en donnant à y des valeurs qui ne sont pas comprises entre deux limites données L et L_1 , on peut satisfaire (abstraction faite des signes) à l'inégalité

$$\frac{Y_r (Y_m)^2}{(Y_n)^3} > \frac{4}{27} ,$$

il sera toujours possible de trouver toutes le solutions entières de l'équation (65), si l'on peut résoudre l'équation $\frac{a}{c} = u^3$, en nombres rationnels, et l'équation $r - m = 3s$, en nombres entiers. En effet les valeurs de y qui ne se trouveront pas parmi les nombres entiers compris entre L et L_1 , fourniront une équation de la forme

$$Dx = Ay^s + By^{s-1} \ldots\ldots + C + \frac{\delta}{\delta_1} ,$$

dans laquelle on pourra réduire la fraction $\frac{\delta}{\delta_1}$ (qui est une fonction de y) aussi petite que l'on voudra, en prenant pour y des nombres entiers qui ne se trouvent pas compris entre deux nouvelles limites l , l_1 ; et partant il faudra donner à y des valeurs entières comprises entre ces limites l , l_1 , ou bien l'on aura l'equation

$$Dx = Ay^s + By^{s-1} \ldots\ldots + C ,$$

qui devra exister en même tems que l'équation (65); et dans les deux cas on pourra trouver toutes les solutions entières de l'équation proposée, par la méthode que nous avons exposée précédemment.

Si, en donnant à y des valeurs non comprises entre deux limites finies l, et l_1, l'on avait (abstraction faite des signes)

$$\frac{Y_r\,(Y_m)^2}{(Y_n)^3} < \frac{4}{27}\ ,$$

on trouverait aisément (par une analyse semblable à celle dont nous venons de faire usage) que pour résoudre complètement dans ce cas par notre méthode l'équation (65), il faudrait pouvoir résoudre l'équation $\frac{b}{a} = u^2$, en nombres rationnels, et l'équation $n - r = 2s$, en nombres entiers.

On pourrait appliquer les mêmes principes aux équations qui sont du quatrième degré par rapport à l'une des inconnues; mais dans ce cas les calculs qu'il faudrait effectuer deviendraient très-longs, et d'ailleurs passé le quatrième degré l'on se trouverait arrêté par l'impossibilité de résoudre les équations algébriques des degrés supérieurs. Nous allons reprendre maintenant cette théorie dans toute sa généralité, à l'aide du théoreme de Lagrange qui sert à exprimer en séries les racines des équations algébriques, et nous exposerons avec plus de detail ce que nous avons à peine indiqué dans l'analyse précédente.

Etant proposée l'équation

$$(66) \ldots\ldots\ldots\ldots \quad a - bx + cx^n = 0\ ,$$

on sait, par le théorème de Lagrange, que lorsqu'on a (abstraction faite des signes)

$$\frac{c\,a^{n-1}}{b^n} < \frac{(n-1)^{n-1}}{n^n}\ ,$$

une des racines de cette équation sera exprimée par la série convergente

$$(67) \ldots \frac{a}{b}\left(1 + \frac{c\,a^{n-1}}{b^n} + \frac{2\,n\,c^2\,a^{2n-2}}{2\,.\,b^{2n}} + \frac{3\,n\,(3\,n-2)\,c^3\,a^{3n-3}}{2\,.\,3\,.\,b^{3n}} + \text{etc.}\right),$$

et les autres $n - 1$ racines seront données par la série convergente

$$(68) \ldots r\left(1 - \frac{a}{(n-1)\,b\,r} - \frac{n\,a^2}{2(n-1)^2\,b^2\,r^2} - \frac{(n-1)\,2\,n\,a^3}{2\,.\,3(n-1)^3\,b^3\,r^3} - \text{etc.}\right),$$

dans laquelle il faut substituer pour r successivement les $n - 1$ racines de l'équation

$$z^{n-1} - \frac{b}{c} = 0 \; .$$

Lorsqu'on a (abstraction faite des signes)

$$\frac{c\,a^{n-1}}{b^n} > \frac{(n-1)^{n-1}}{n^n} \;,$$

les n racines de l'équation proposée seront exprimées par la série convergente

$$(69) \ldots r\left(1 - \frac{b\,r}{n\,a} + \frac{(3-n)\,b^2\,r^2}{2\,.\,n^2\,a^2} - \frac{(4-n)(4-2n)\,b^3\,r^3}{2\,.\,3\,.\,n^3\,a^3} + \text{etc.}\right),$$

dans laquelle il faudra substituer pour r successivement les n racines de l'équation

$$z^n + \frac{a}{c} = 0 \; .$$

Il résulte de là, que lorsque (abstraction faite de signes) l'on a

$$\frac{c\,a^{n-1}}{b^n} < \frac{(n-1)^{n-1}}{b^n} \;,$$

l'équation (66) aura autant de racines réelles qu'il y en a dans les deux équations

$$b\,z - a = 0 \;,\quad c\,z^{n-1} - b = 0 \;,$$

et que lorsque (abstractiou faite des signes) on a

$$\frac{c\,a^{n-1}}{b^n} > \frac{(n-1)^{n-1}}{n^n} \;,$$

il y aura autant de racines réelles qu'il y en a dans l'équation

$$c\,z^n + a = 0 \; .$$

Maintenant si l'on suppose

$$a = -\alpha \ , \ b = -\beta \ , \ c = \gamma \ ,$$

(α, β, γ, étant trois quantités positives) et si l'on prend pour n un nombre impair quelconque, on aura les deux équations

$$\gamma z^{n-1} + \beta = 0 \ , \ \gamma z^n - \alpha = 0 \ ,$$

dont la première aura toutes ses racines imaginaires, tandis que la seconde n'aura qu'une seule racine réelle; et par conséquent l'équation

$$(70) \ldots\ldots\ldots\ldots \gamma x^n + \beta x - \alpha = 0 \ ,$$

(dans laquelle α, β, γ, sont trois quantités positives) aura toujours une seule racine réelle, quelle que soit la valeur des coefficiens α, β, γ.

A présent si dans l'équation (70) on fait, par exemple,

$$\alpha = p y^{mn} + q \ , \ \beta = r y^{mn-2} + s \ , \ \gamma = t \ ,$$

(p, r, t, étant trois quantités positives) on aura, après les substitutions,

$$(71) \ldots\ldots p y^{mn} + q = (r y^{mn-2} + s) x + t x^n \ ,$$

et par suite (abstraction faite des signes) la quantité

$$\frac{c a^{n-1}}{b^n} = \frac{\gamma(-\alpha)^{n-1}}{(-\beta)^n} = \frac{t(-p y^{mn} - q)^{n-1}}{(-r y^{mn-2} - s)^n}$$

sera plus grande ou plus petite que $\frac{(n-1)^{n-1}}{n^n}$, selon le rapport de m à n.

Soit $nm > 2n$, alors on pourra trouver deux limites L et L_1, de y telles, qu'en prenant pour y des nombres entiers quelconques qui ne soient pas compris entre ces limites, on ait toujours (abstraction faite des signes)

$$(72) \ldots\ldots\ldots \frac{t(-p y^{mn} - q)^{n-1}}{(-r y^{mn-2} - s)^n} < \frac{(n-1)^{n-1}}{n^n} \ .$$

Lorsque cette inégalité est satisfaite, pour trouver toutes les valeurs de x qui résolvent l'équation (71), il faudra faire usage des deux séries (67), (68); et en substituant dans la première de ces séries les valeurs

$$a = -\alpha = -py^{mn} - q \quad , \quad b = -\beta = -ry^{mn-2} - s \quad , \quad c = \gamma = t \quad ,$$

on aura

$$(73)\ldots x = \left(\frac{py^{mn}+q}{ry^{mn-2}+s}\right)\left\{\begin{array}{l} 1 + \dfrac{t(-py^{mn}-q)^{n-1}}{(-ry^{mn-2}-s)^{n}} + \dfrac{2n\,t^2(-py^{mn}-q)^{2n-2}}{2(-ry^{mn-2}-s)^{2n}} \\ + \dfrac{3n(3n-2)t^3(-py^{mn}-q)^{3n-3}}{2\,.\,3\,(-ry^{mn-2}-s)^{3n}} \ldots + \text{etc.} \end{array}\right\} .$$

Mais comme par hypothèse l'on a $mn > 2n$, ou bien $m > 2$, et que chaque terme de la série précédente peut se réduire aussi petit que l'on voudra en donnant à y des valeurs entières qui ne soient pas comprises entre deux limites L, L_1, facilement assignables, on aura toujours (lorsque y n'est pas compris entre ces limites) une équation de la forme

$$Nx = Ay^2 + By + C + \frac{\delta}{\delta_1} \quad ,$$

dans laquelle N, A, B, C, sont des nombres entiers, et $\frac{\delta}{\delta_1}$ est une fraction plus petite que l'unité; d'où l'on déduira l'équation

$$Nx = Ay^2 + By + C \quad ,$$

qui devra exister en même tems que l'équation (71), et qui servira à trouver toutes les valeurs de y non comprises entre les limites L, L_1; mais comme d'ailleurs les valeurs de y comprises entre ces limites peuvent se trouver séparément, l'équation (71) sera résolue complètement quant à la série (67); et si l'on suppose que les coefficiens de l'équation (71) restent toujours positifs, quelle que soit la valeur de y, il est clair que l'équation (71) ne fournira qu'une seule racine réelle pour x, qui sera représentée par l'équation (73); ainsi dans ce cas l'équation (71) sera résolue complètement, pourvu que l'inégalité (72) soit satisfaite.

Si les coefficiens de l'équation (71) ne sont positifs, que pour des valeurs de y comprises entre les limites L, L_1, on pourra, par l'analyse précédente, trouver toutes les solutions de cette équation qui correspondent à des valeurs entières de y comprises entre L et L_1.

Il est clair que si l'équation

$$py^{mn} + q = (ry^{mn-2} + s)x + tx^n ,$$

est résoluble par la méthode que nous venons d'exposer, on pourra résoudre aussi l'équation plus générale

$$(74)\ldots py^{mn}+p_1y^{mn-1}+p_2y^{mn-2}\ldots+q_1y+q=(ry^{mn-2}+r_1y^{mn-3}\ldots+s_1y+s)x+tx^n ,$$

dans laquelle les coefficiens

$$p_1 \ , \ p_2 \ , \ \ldots\ldots \ q_1 \ , \ q \ , \ r \ , \ r_1 \ \ldots\ldots \ s_1 \ , \ s \ , \ t \ ,$$

sont des nombres rationnels quelconques. En effet l'on pourra toujours, dans chaque coefficient de x, rendre le terme qui contient la puissance la plus élevée de y plus grand que la somme de tous les autres, et alors les conditions d'inégalité ne porteront que sur les termes qui contiennent ces plus grandes puissances; et comme les autres conditions ne regardent que ces termes, il en résulte que si l'équation (71) est résoluble, l'équation (74) sera résoluble aussi.

Si au lieu de l'équation (74), on voulait résoudre en nombres entiers l'équation plus générale

$$ay^{mn} + by^{mn-1} + cy^{mn-2}\ldots + d = (ey^{mn-p} + fy^{mn-p-1}\ldots + g)x + hx^n ,$$

dans laquelle les coefficiens e, h, sont positifs, il suffirait d'avoir $m > p$, pour en obtenir toutes les solutions entières, ou du moins toutes les solutions entières positives, par notre méthode.

En général étant proposée l'équation à coefficiens rationnels

$$ay^n + by^{n-1}\ldots + cy + d = (ey^p + fy^{p-1}\ldots + g)x + hx^m ,$$

on pourra, par la méthode que nous avons exposée, trouver toutes ses solutions

entières pourvu que le produit eh reste toujours positif et que l'on ait (abstraction faite des signes)

$$\frac{h(ay^n + by^{n-1} \ldots + d)^{m-1}}{(ey^p + fy^{p-1} \ldots + g)^m} < \frac{(m-1)^{m-1}}{m^m} .$$

Ainsi par exemple on pourra toujours trouver toutes les solutions entières de l'équation

$$ay^7 + by^6 + cy^5 + dy^4 + ey^3 + fy^2 + gy + h$$
$$= x(iy^6 + ky^5 + ly^4 + my^3 + ny^2 + py + q) + rx^5 ,$$

pourvu que le produit ir soit positif.

Lorsque dans l'équation (70) le coefficient β est négatif, l'équation

$$\gamma z^{n-1} + \beta = 0 ,$$

aura deux racines réelles, et alors si la condition

$$\frac{\gamma \alpha^{n-1}}{\beta^n} < \frac{(n-1)^{n-1}}{n^n}$$

est satisfaite (abstraction faite des signes) outre la série (67), il faudra considérer la série (68), qui fournira deux nouvelles racines réelles de l'équation (70), en y substituant les valeurs des coefficiens. Mais afin que notre méthode puisse s'appliquer à la série (68) il faudra que l'on ait

$$\frac{\beta}{\gamma} = -(a^{n-1} y^{mn-m} + b y^{mn-m-1} \ldots\ldots + \text{etc.}) ,$$

car alors l'équation

$$z^{n-1} + \frac{\beta}{\gamma} = 0 ,$$

donnera les deux valeurs réelles

$$z = \pm(ay^m + by^{m-1} + \text{etc.}) ,$$

et ces deux valeurs étant combinées avec la série (68), fourniront toutes les solutions entières de l'équation proposée.

Si l'on a, dans l'équation

$$a - bx + cx^n = 0 \quad ,$$

(abstraction faite des signes)

$$\frac{c a^{n-1}}{b^n} > \frac{(n-1)^{n-1}}{n^n} \quad ,$$

on ne pourra plus faire usage des deux séries (67) et (68) pour obtenir les valeurs de x, car dans ce cas ces deux séries deviendraient divergentes: alors il faudra recourir à la série (69) qui renferme le radical $\left(\frac{-a}{c}\right)^{\frac{1}{n}}$, et il est clair que l'équation proposée aura une ou deux racines réelles selon que le nombre n sera impair ou pair; en observant cependant que lorsque n sera pair, et que la fraction $\frac{a}{c}$ sera positive, l'équation $a - bx + cx^n = 0$, n'aura aucune racine réelle, tant que l'inégalité précédente sera satisfaite.

Maintenant si l'on suppose que les coefficiens a, b, c soient des fonctions de y, il faudra, pour appliquer les principes que nous avons exposés précédemment, que l'on ait toujours

$$\frac{c a^{n-1}}{b^n} > \frac{(n-1)^{n-1}}{n^n} \quad ,$$

et ensuite

$$-\frac{a}{c} = -\frac{dy^{mn} + ey^{mn-1} \ldots\ldots + py + q}{c} = g^n y^{mn} + h y^{mn-1} + \text{etc.} \; ,$$

car alors on trouvera

$$\sqrt[n]{\frac{-a}{c}} = g y^m + k y^{m-1} + l y^{m-2} \;\ldots\ldots + \text{etc.} \quad ,$$

et en substituant cette valeur dans la série (69), on parviendra aisément à la résolution complète en nombres entiers de l'équation proposée.

En général étant proposée l'équation à deux inconnues

$$(75)\ldots\left\{\begin{array}{c} x^n(ay^m+by^{m-1}\ldots+cy+d)+(ey^r+fy^{r-1}\ldots+hy+i)x \\ -(ky^p+ly^{p-1}\ldots qy+s) \end{array}\right\}=0\,,$$

on pourra toujours la résoudre complètement en nombres entiers dans les cas suivans.

1.° Lorsque n étant un nombre impair, et les deux termes ay^m, ey^r, ayant le même signe on peut trouver deux limites finies L, L_1, telles, qu'en prenant pour y des valeurs entières qui ne soient pas comprises entre ces limites, on ait toujours (abstraction faite des signes)

$$(76)\ldots\ldots\ \frac{ak^{n-1}\,y^{m+np-p}}{e^n\,y^{rn}} < \frac{(n-1)^{n-1}}{n^n}\,.$$

2.° L'équation (75) sera résolue complètement lorsque (n étant un nombre entier quelconque, et l'inégalité (76) étant satisfaite, mais les deux termes ay^m, ey^r, n'ayant pas le même signe) on pourra résoudre l'équation $\frac{e}{a}=u^{n-1}$, en nombres rationnels, et l'équation $r-m=(n-1)z$, en nombres entiers.

3.° L'équation (75) pourra être résolue complètement en nombres entiers, (quels que soient les signes des termes ay^m, ey^r,) lorsqu'il sera possible de trouver deux limites finies L, L_1, telles qu'en prenant pour y des valeurs entières non comprises entre ces limites, on ait toujours

$$(77)\ldots\ldots\ \frac{ak^{n-1}\,y^{m+np-p}}{e^n\,y^{rn}} > \frac{(n-1)^{n-1}}{n^n}\,,$$

et que l'on pourra résoudre l'équation $\frac{k}{a}=u^n$, en nombres rationnels, et l'équation $p-m=nz$, en nombres entiers.

4.° Lorsque l'inégalité (77) étant toujours satisfaite, l'exposant n sera un nombre pair, et les deux termes ky^p, ay^m, auront des signes différens, on pourra trouver toutes les solutions entières de l'équation (75).

Il faut observer ici que souvent les conditions précédentes ne sont satisfaites, dans l'équation (75), qu'entre des limites données des inconnues; alors au lieu de trouver toutes les solutions entières de l'équation proposée, on aura seulement, par notre méthode, les solutions comprises entre deux limites connues. Ainsi, par exemple, quelquefois on trouvera toutes les solutions positives de l'équation (75), sans que l'on puisse obtenir les solutions négatives.

Si dans l'équation (75) on fait $n = 2$, et si l'on suppose que l'inégalité (76), qui dans le cas actuel se réduit à celle-ci

$$4\,a\,k\,y^{m+p} \;<\; e^2\,y^{2r}\quad,$$

soit toujours satisfaite en donnant à y des valeurs non comprises entre deux limites finies L, L_1, il est clair que l'on pourra résoudre complètement l'équation proposée a l'aide des deux séries (67) et (68), car la seconde n'aura, dans le cas de $n = 2$, qu'une seule valeur qui sera toujours rationnelle.

Lorsque l'on a, au contraire, (abstraction faite des signes)

$$4\,a\,k\,y^{m+p} \;>\; e^2\,y^{2r}\quad,$$

en donnant à y des valeurs quelconques non comprises entre deux limites finies l, l_1, il faudra faire usage de la série (69), et afin qu'elle ne contienne aucun terme irrationnel, on devra pouvoir résoudre l'équation $\frac{k}{a} = z^2$, en nombres rationnels, et l'équation $p - m = 2s$, en nombres entiers. Il est clair que ces deux équations se réduisent aux deux suivantes $a\,k = u^2$, $p + m = 2t$, qui sont celles que nous avons déjà obtenues.

Les deux équations précédentes doivent être résolubles dans le cas que le terme $a\,k\,y^{m+p}$ soit positif, mais lorsqu'il est négatif, et que l'on a

$$4\,a\,k\,y^{m+p} \;>\; e^2\,y^{2r}\quad,$$

la série (69) aura deux valeurs imaginaires; et partant les valeurs de x qui

correspondent à des valeurs de y non comprises entre des limites finies L, L_1, seront toujours imaginaires; mais comme les valeurs entières de y comprises entre ces limites, se déterminent aisément, on aura résolu complètement l'équation proposée, sans qu'il soit nécessaire de satisfaire aux deux conditions que nous avons trouvées précédemment.

Soit maintenant $n = 3$ dans l'équation (75), et supposons que l'inégalité (76) soit satisfaite, dans le cas actuel elle se réduira à l'autre

$$\frac{a h^2 y^{m+2p}}{e^3 y^{3r}} < \frac{4}{27} ,$$

et il faudra faire usage des deux séries (67) et (68), pour obtenir les valeurs entières de x qui résolvent l'équation proposée. A présent si dans la série (67), on substitue les valeurs des coefficiens de l'équation (75), on aura une série convergente qui fournira, à l'aide de notre méthode, toutes les solutions entières de l'équation (75) qui correspondent à l'une des formes des racines. Pour obtenir toutes le autres solutions entières, il faut considérer les valeurs de x fournies par la série (68); et comme celle-ci, lorsque $n = 2$, contient le radical $\left(\frac{b}{c}\right)^{\frac{1}{2}}$ qui, pour l'équation (75), se transforme dans l'autre

$$(78) \ldots\ldots\ldots \left(-\frac{ey^r + fy^{r-1} \ldots\ldots + i}{ay^m + by^{m-1} \ldots\ldots + d}\right)^{\frac{1}{2}} ,$$

il faudra, pour y appliquer notre méthode, que l'on ait l'équation $-\frac{e}{a} = u^2$, en nombres rationnels, et l'équation $r - m = 2s$, en nombres entiers, et l'on voit que dans ce cas l'équation (75) sera résolue complètement. Mais si la quantité comprise entre les crochets dans le radical (78) demeure toujours négative, pour des valeurs quelconques de y non comprises entre deux limites finies L, L_1, il est clair que le radical (78) deviendra imaginaire dans les mêmes circonstances; alors la série (68) ne donnera que des valeurs imaginaires de x, excepté pour des valeurs entières de y comprises entre les limites L, L_1, valeurs que l'on considérera séparément. Ainsi dans ce cas l'équation (75) sera

résolue complètement à l'aide de la série (67), pourvu que l'inégalité

$$27\ a\,k^2\,y^{m+2p} < 4\,c^3\,y^{3r}$$

soit satisfaite, et sans qu'il soit nécessaire de vérifier aucune autre condition.

Si l'on avait au contraire

$$27\ a\,k^2\,y^{m+2p} > 4\,c^3\,y^{3r} \quad ,$$

il faudrait recourir à la série (69), et comme celle-ci contient le radical $\left(\frac{a}{c}\right)^{\frac{1}{3}}$ qui, pour l'équation (75), devient

$$-\left(\frac{ky^p + ly^{p-1} \ldots\ldots + s}{ay^m + by^{m-1} \ldots\ldots + d}\right)^{\frac{1}{3}} ,$$

on devra, afin que notre méthode soit applicable, pouvoir résoudre l'équation $\frac{k}{a} = u^3$, en nombres rationnels, et l'équation $p - m = 3s$, en nombres entiers; et si ces deux conditions sont satisfaites, l'équation (75) sera résolue complètement.

L'analyse précédente montre qu'en appliquant la série de Lagrange aux équations indéterminées qui sont du second ou du troisième degré par rapport à l'une des inconnues, on rencontre les mêmes conditions que la forme des racines nous avait fait découvrir, et que même l'on trouve de nouveaux cas de solution. En appliquant notre méthode aux équations des degrés supérieurs, on trouve la résolution complète d'un grand nombre d'équations indéterminées, qu'on n'aurait pu traiter d'aucune manière par les méthodes connues.

Si au lieu de l'équation (66) on avait l'autre

$$a - b\,x^m + c\,x^{m+n} = 0 \quad ,$$

on sait que la série (67) contiendrait la radical $\left(\frac{a}{b}\right)^{\frac{1}{m}}$, et alors si a, b, c,

étaient des fonctions de y, la première série aussi fournirait deux équations de condition de la forme

$$\frac{h}{e} = u^m \quad , \quad p - r = ms \quad ,$$

dont la première devrait être résoluble en nombres rationnels, et la seconde en nombres entiers; et il est clair que ces équations deviennent identiques dans le cas de $m = 1$.

En général étant proposé de résoudre en nombres entiers l'équation à deux inconnues

$$a + bx + cx^2 \ldots\ldots + dx^n = 0 \quad ,$$

dans laquelle les coefficiens a, b, c, ... d, sont des polynomes en y entiers et rationnels, à coefficiens rationnels, on réduira d'abord tous ces coefficiens au dénominateur commun, et puis on les multipliera par ce dénominateur pour les rendre tous entiers; ensuite on cherchera par le théorème de Lagrange les diverses séries qui représentent les n valeurs de x, et l'on trouvera toutes les conditions auxquelles doivent satisfaire les termes qui dans les coefficiens a, b, c, ... d, contiennent les plus grandes puissances de y, afin que l'équation proposée soit résoluble par notre méthode, en observant que lorsque ces conditions, qui regardent les termes contenant les plus grandes puissances de y, seront satisfaites dans une équation donnée, on pourra changer d'une manière quelconque les autres termes, qui ne contiennent pas les plus grandes puissances de y, et toutes les équations que l'on obtiendra de cette manière seront toujours résolubles.

Pour résoudre en nombres entiers l'équation

$$F(x \;,\; y) = 0 \quad ,$$

(dans laquelle $F(x, y)$ exsprime une fonction quelconque entière et rationnelles des inconnues x, et y, à coefficiens rationnels) il peut être utile de considérer quelques puissances de l'une des inconnues comme des coefficiens algébriques; de cette manière on réduit l'équation proposée à une autre plus



simple, et lorsqu'en résolvant cette nouvelle équation par la série de Lagrange, notre méthode est encore applicable, on obtiendra la résolution complète de l'équation proposée. On pourrait aussi dans plusieurs cas résoudre complètement de la même manière des équations contenant trois ou un plus grand nombre d'inconnues; mais ces recherches exigeraient de trop longs développemens, et ne sauraient trouver place ici.

En général au lieu de chercher par le théorème de Lagrange l'expression en série des racines de l'équation proposée, on peut chercher le développement d'une fonction quelconque des inconnues. Ainsi, par exemple, étant proposé de résoudre en nombres entiers l'équation à deux inconnues

$$\varphi(x\ ,\ y) = 0\ ,$$

si l'on peut trouver une fonction entière $F(x\,,y)$ des mêmes inconnues telle, qu'étant développée par les puissances descendantes d'une autre fonction entière $f(x\,,y)$ de cette manière

$$F(x\,,y) = B + \frac{B_1}{f(x\,,y)} + \frac{B_2}{(f(x\,,y))^2}\ \ldots\ldots + \text{etc.}\ ,$$

le rapport de deux coefficiens consécutifs demeure toujours positif, et ne puisse jamais atteindre une limite entière A, on trouvera $2B$ pour la limite de $F(x\,,y)$, lorsqu'on donnera à la fonction $f(x\,,y)$, une valeur égale ou plus grande que $2A$; alors en éliminant une des inconnues entre l'équation

$$\varphi(x\ ,\ y) = 0\ ,$$

et l'une quelconque des suivantes

$$F(x\,,y) = 0\ ,\ F(x\,,y) = 1\ ,\ F(x\,,y) = 2\ ,\ \ldots\ F(x\,,y) = 2B - 1\ ,$$

ou bien entre la même équation

$$\varphi(x\ ,\ y) = 0\ ,$$

et l'une des suivantes

$$f(x,y)=0\ ,f(x,y)=1\ ,\ f(x,y)=2\ ,\ \ldots f(x,y)=2A-1\ ,$$

on aura un nombre $2(A+B)$ d'équations à une seule inconnue, dont les racines entières exprimeront toutes les solutions entières de l'équation

$$\varphi(x\ ,\ y)=0\ .$$

Nous avons supposé que tous les coefficiens B, B_1, B_2, ... etc., avaient le même signe; mais s'ils avaient des signes alternatifs, en faisant $f(x,y)>2A$, on n'aurait plus $F(x,y)<2B$. Cependant en faisant $f(x,y)>AB$, la valeur de $F(x,y)$, serait toujours comprise entre B et $B-1$, et l'on serait assuré qu'il faudrait avoir en même tems

$$F(x\ ,\ y)=B\ ,\ \varphi(x\ ,\ y)=0\ ,$$

ou bien l'équation

$$\varphi(x\ ,\ y)=0\ ,$$

devrait exister en même tems que l'une des suivantes

$$f(x,y)=0\ ,f(x,y)=1\ ,f(x,y)=2\ ,\ \ldots f(x,y)=AB\ ,$$

et l'équation proposée serait résolue complètement.

L'esprit de la méthode que nous avons exposée dans ce mémoire consiste en ceci; qu'étant proposé de résoudre en nombres entiers l'équation à deux inconnues

$$F(x\ ,\ y)=0\ ,$$

on devra chercher une fonction entière des inconnues $f(x,y)$, telle que l'on ait l'équation

$$(79)\ \ldots\ldots\ldots f(x\ ,\ y)=f_1(x\ ,\ y)+\frac{\delta}{\delta_1}\ ,$$

dans laquelle $f_1(x, y)$ est aussi une fonction entière de x et y, et δ, δ_1, sont deux fonctions des mêmes inconnues, telles qu'en prenant en même tems (abstraction faite des signes) pour x des valeurs entières non comprises entre les deux limites finies $+L$ et $-L$, et pour y des valeurs entières non comprises entre les deux limites finies $+L$, et $-L_1$, on ait toujours (abstraction faite des signes) $\frac{\delta}{\delta_1} < 1$.

Maintenant il est clair qu'en prenant en même tems pour x des valeurs non comprises entre $+L$ et $-L$, et pour y des valeurs non comprises entre $+L_1$ et $-L_1$, l'équation (79) se réduira à l'autre

$$(80) \ldots\ldots\ldots f(x, y) = f_1(x, y),$$

qui devra exister en même tems que l'équation $F(x, y) = 0$, et qui donnera, par l'élimination, toutes les solutions de l'équation proposée, non comprises en même tems entre les limites trouvées précédemment. Mais si les deux inconnues x et y, n'étaient pas comprises à la fois entre ces limites, l'équation (80) n'aurait plus lieu; cependant alors comme l'on devrait avoir (abstraction faite des signes) $x < \pm L$, ou $y < \pm L_1$, on poserait les équations

$$x = 0, x = \pm 1, x = \pm 2, \ldots\ldots x = \pm (L - 1),$$

ou bien les autres

$$y = 0, y = \pm 1, y = \pm 2, \ldots\ldots y = \pm (L_1 - 1),$$

et on pourrait éliminer une inconnue entre l'une quelconque de ces équations, et l'équation

$$F(x, y) = 0,$$

qui serait de cette manière résolue complètement, puisqu'ayant trouvé d'abord les valeurs entières de x non comprises entre les limites $-L$ et $+L$, et les valeurs entières de y non comprises entre les limites $-L_1$ et $+L_1$, et



puis les solutions comprises entre ces limites, on aura toutes les solutions entières possibles de l'équation proposée.

Les méthodes que nous avons exposées dans le mémoire précédent et dans celui-ci, contiennent les premiers élémens d'une théorie générale sur la résolution complète des équation indéterminées qui ont un nombre fini de solutions entières. Cette théorie présente de grandes difficultés lorsqu'on veut l'appliquer aux cas particuliers, et demande des recherches fort laborieuses qui ne sauraient trouver place ici, mais que nous esperons pouvoir exposer dans une autre circonstance.

MÉMOIRES DE MATHÉMATIQUE DONT LA RÉDACTION EST PRESQUE ACHEVÉE ET QUI FAIRONT PARTIE DES VOLUMES SUIVANS; AVEC L'ÉNONCÉ DE QUELQUES-UNS DES PROBLÈMES RÉSOLUS DANS CHAQUE MÉMOIRE.

I. *Mémoire sur les transcendantes numériques.*

Problèmes.

1.° Etant donné un nombre quelconque n, trouver directement et sans tatonnement, par une opération algébrique, un nombre premier p qui soit plus grand que n.

2.° Etant donnée la série des nombres premiers successifs

$$1 \, , \, 2 \, , \, 3 \, , \, 5 \, , \, 7 \, , \, 11 \, , \, 13 \, , \, \ldots\ldots \, p \, ,$$

(dans laquelle p exprime le plus grand de ces nombres premiers) déterminer le nombre premier p_1, qui suit immédiatement le nombre premier p, en fonction des nombres

$$1 \, , \, 2 \, , \, 3 \, , \, 5 \, , \, 7 \, , \, 11 \, , \, 13 \, , \, \ldots\ldots \, p \, ,$$

en termes finis.

3.° Etant donnés deux nombres entiers quelconques a et b, exprimer en termes finis, en fonction de a et b, la somme des puissances n.mes de ceux, parmi les nombres entiers compris entre a et b, qui ont seulement un nombre m de facteurs.



II. *Memoire sur les congruences du troisième et du quatrième degré, et des degrés supérieurs.*

Problêmes.

1.° Soit p un nombre premier de la forme $6n + 1$; on aura toujours $4p = a^2 + 27b^2$, et si l'on cherche les racines entières, communes aux deux congruences

$$y^{6n-3} + 2ny^{6n-6} + \frac{4}{2}(2n)^2 y^{6n-9} \frac{4 \cdot 7}{2 \cdot 3}(2n)^3 y^{6n-12} \ldots + \text{etc.} \equiv 0 \pmod{p},$$

$$y^{6n-1} - (6n)^3 y^{6n-2} + (6n)^4 y^{6n-3} - (6n)^7 y^{6n-4} + (6n)^8 y^{6n-5} - \text{etc.} \equiv 0 \pmod{p},$$

on trouvera, en général, pour facteur commun une congruence du degré m ; maintenant il s'agit de trouver le rapport qui doit exister entre a et m, afin que la congruence

$$x^3 + 2 \equiv 0 \pmod{p},$$

soit résoluble.

2.° Soit p un nombre premier quelconque : on pourra toujours résoudre l'équation $4p = x^2 + zy^2$, en nombres entiers d'une infinité de manières. Maintenant, parmi toutes les valeurs entières de z, il s'agit d'en déterminer une, directement et par une méthode générale, telle que x et y, soient deux résidus cubiques de p, quel que soit le nombre premier p qui doit rester indéterminé.

3.° En exprimant par p un nombre premier quelconque, il s'agit de déterminer les valeurs de p dans lesquelles parmi les résidus cubiques de p moindres que p, il y en aura toujours au moins un de la forme $a^3 + b^3$; a et b, étant deux nombres entiers différens de zéro.

4.° Trouver toutes les solutions entières de l'équation indéterminée.

$$\left\{\begin{array}{l} 9z^6y^2+9z^6y-6z^5-6z^3-(y^2+y-5)\big(12z^7-12z^6(y^2-u^3-2)+12z^4(y^2-u+1)\big) \\ +4z^2(y^2-y-5)\big(3z^2y^4-3y^2z^2(u^3+u+1)+3z^2(u^4-u^3+2u-2)+z^4(z^2-y^2+u^3+2)^2\big) \\ +4z^2(y^2+y-5)(z^2-y^2+u^3+2)^2\big((z-y^2+u^3+2)^2-z^4\big) \\ -(4y^4+2y^3-10y^2)(z^4+2z^2y^2-2z^2u+2z^2-2uy^2+2y^2-2u+y^4+u^2+1) \end{array}\right\}$$

$$=\left\{\begin{array}{l} 45z^6-6z^3u+6z^3-3yz^4-6z^2y^3+6z^2uy-6z^2y+6uy^3-6y^3+6uy-3y^5-3u^2y-3y \\ -\big(4z^4-4z^3(y^2-u^3-2)+4z^2(y^2-u+1)-4zy^4+4zy^2(u^3+u+1)-4z(u^4-u^3+2u-2)\big)(z^2+y^2-u+1) \end{array}\right\}$$

III. *Mémoire sur les intégrales définies qui dépendent de la théorie des nombres.*

Problèmes.

1.° Déterminer les valeurs des coefficiens de l'équation

$$y^{n-1} + Ay^{n-2} + By^{n-3} \ldots\ldots + C = 0,$$

qui a pour racines les $n - 1$ quantités

$$\frac{\cos\frac{2b\pi}{n}}{\left(\sin\frac{a\pi}{n}\right)^2}, \quad \frac{\cos\frac{4b\pi}{n}}{\left(\sin\frac{2a\pi}{n}\right)^2}, \quad \frac{\cos\frac{6b\pi}{n}}{\left(\sin\frac{3a\pi}{n}\right)^2}, \quad \ldots\ldots \quad \frac{\cos 2(n-1)\frac{b\pi}{n}}{\left(\sin (n-1)\frac{a\pi}{n}\right)^2};$$

dans lesquelles a, b, n, sont trois nombres entiers quelconques qui n'ont pas de commun diviseur.

2°. Déterminer les conditions qui rendent la formule

$$\sum_{x=1}^{x=a} \frac{\sin(2b+n)\frac{x\pi}{a}}{\sin\frac{x\pi}{a}} + \left\{ \operatorname{tang}\left(\frac{n-1}{2} + \frac{1}{2}\sum_{x=1}^{x=n} \frac{\sin(2b-a)\frac{x\pi}{n}}{\sin\frac{ax\pi}{n}}\right)\frac{\pi}{a}\right\}^{\frac{1}{2}}$$

$$+ \sum_{x=1}^{x=n} \frac{2an\sin(2b-a)\frac{x\pi}{n} - \sin\frac{ax\pi}{n} \cdot \sqrt{\operatorname{tang}\frac{x\pi}{a}}}{2n\sin\frac{ax\pi}{n}}$$

$$+ \sum_{x=0}^{x=n} \frac{\sin(ax+b-2anx-2bn)\frac{\pi}{n}}{2n\sin(ax+b)\frac{\pi}{n}} \cdot \sqrt{\operatorname{tang}\frac{x\pi}{a}}$$

$$+ \sum_{x=1}^{x=n} \frac{\left(1 - \cos\frac{2\pi}{n}\cos\frac{2x^2\pi}{n} + \cos\frac{4\pi}{n}\right)\sin\frac{2x^2\pi}{n}}{2\left(1 + 2\cos\frac{2\pi}{n}\cos\frac{2x^2\pi}{n}\right)\cos\frac{2x^2\pi}{n} + 2\cos\frac{4\pi}{n}}$$

égale à une quantité finie, sans que les quantités a, b, n, soient données en nombres.

IV. *Mémoire sur la résolution des équations numériques.*

Problème.

Etant donnée une équation numérique quelconque à coefficiens rationnels, trouver, parmi ses racines, toutes celles qui peuvent être construites par la règle et le compas, et cela sans le secours de la théorie des nombres, ni de la théorie des lignes courbes, mais seulement à l'aide des principes élémentaires de la théorie des équations algébriques.

V. *Mémoire sur le calcul des probabilités.*

Problème.

Deux joueurs jouant aux échecs, et les pièces étant disposées d'une manière quelconque sur l'échiquier, supposons que chaque joueur joue chaque coup de la meilleure manière possible; maintenant il s'agit d'exprimer en série convergente le nombre des coups après lesquels l'un des deux joueurs recevra nécessairement échec et mat.

VI. *Mémoire sur la comparaison des différens ordres d'irrationalité.*

Problème.

Etant donnée une équation algébrique quelconque, et l'une de ses racines irrationnelles, en combien de facteurs algébriques peut-on décomposer l'équation proposée?

MÉMOIRES DE PHYSIQUE QUI PARAÎTRONT DANS LES VOLUMES SUIVANS, DÈS QUE L'ON AURA RÉPÉTÉ QUELQUES-UNES DES EXPÉRIENCES LES PLUS IMPORTANTES.

I. *Mémoire sur la flamme et sur les mouvemens que la chaleur produit dans les corps soumis à son action.* (*)

II. *Mémoire sur quelques phénomènes de diffraction de la lumière et de la chaleur.* (**)

III. *Mémoire sur la formation du phosphore dans les animaux.*

IV. *Mémoire sur l'influence du tems dans les phénomènes physiques.*

V. *Mémoire sur le maximun de densité dans les liquides.*

VI. *Mémoire sur les odeurs.* (***)

VII. *Mémoire sur la transparence des corps.*

VIII. *Mémoire sur la scintillation des astres et des corps terrestres.*

(*) Voyez le N.° 73 de l'*Antologia di Firenze*.

(**) Voyez le N.° 88 de l'*Antologia*.

(***) Voyez le N.° 77 de l'*Antologia*.

ERRATA.

PAGES.	LIGNES.	FAUTES.	CORRECTIONS.
IX	2	peut-être	peut-être
2	6	d'effectuer,	, d'effectuer
5	8	M.r	M.
5	2 en remont.	on trouvera	(pourvu que l'on suppose $x_0 = x$) on trouvera
6	5	en faisant	en faisant toujours
6	7	$a_{x_e-x_{s+1}}$	$a_{x_s-x_{s+1}}$.
7	10	déja	déjà
8	9 en rem.	u ;	u ,
12	8 en rem.	porvu	pourvu
15	12 en rem.	déja	déjà
16	5	M.r	M.
16	19	a	à
16	11 en rem.	M.r	M.
18	2	lorsqne	lorsque
24	9	$\cos \frac{nx}{r}$	$\cos \frac{mx}{r}$
24	dernière	$V =$	$v =$
28	7 en rem.	Newtou	Newton
29	7	$\cos \frac{x}{r}$	$\cos \frac{x}{r}$,
31	13	permanente	permanent
31	9 en rem.	lineaire	linéaire
39	5	puisque	, puisque
40	14	a	à
44	17	géometres	géomètres

PAGES.	LIGNES.	FAUTES.	CORRECTIONS.
48	16 en rem.	admettait	admettaient
52	14	$\sum_{z=0}^{z=\infty}$	$\sum_{z=1}^{z=\infty}$
55	11 en rem.	équations ;	équations,
56	10	methode	méthode
57	17	à x	à x,
57	19	diviseur	diviseur,
58	16	équations	équations,
58	21	$+ pu$	$- pu$
58	5 en rem.	considèrerons	considérerons
58	4 en rem.	specialement	spécialement
63	4	congeuence	congruence
65	2	Ψ	Φ
65	5	Ψ	Φ
67	7 en rem.	y	Y
67	dernière	$(A^{n-1} v^{n-1} - 1)^2 - 1))$, ...	$(A^{n-1} v^{n-1} - 1)^2 - 1)$,
73	3	sur	sur les
76	14	équation	équations
77	11 en rem.	congrnence	congruence
77	7 en rem.	$\frac{d\varphi}{dx} \equiv 0 \pmod{p}$; ..... etc.	$\frac{d\varphi}{dy} \equiv 0 \pmod{p}$; ..... etc.
80	1	denx	deux
80	3	speciales	spéciales
80	14	$\sin 2\left(1.2.3...(p-1)+\frac{1.2.3...(p-1)+1}{2p}\right)\pi$	$\sin 2\left(1.2.3...(p-1)+1-\frac{1.2.3...(p-1)+1}{2p}\right)\pi$

PAGES.	LIGNES.	FAUTES.	CORRECTIONS.
81	5	expression	expressions
81	11	au	ou
82	9 en rem.	$+\cos\left(\frac{2(m-1)\varphi\pi}{m}+\sqrt{-1}\sin\frac{2(m-1)\varphi\pi}{m}\right)\ldots$	$+\left(\cos\frac{2(m-1)\varphi\pi}{m}+\sqrt{-1}\sin\frac{2(m-1)\varphi\pi}{m}\right)$
83	3 en rem.	tems	terme
83	dernière	nombre	membre
85	6 en rem.	congruencc	congruence
88	3	données,	données
88	3 en rem.	$\sum_{u=0}^{u=4}$	$\sum_{u=1}^{u=4}$
90	7	répetés	répétés
93	3	$\sum_{y=1}^{y=1}$	$\sum_{y=1}^{y=n}$
95	3	$-2\sum_{u=1}^{u=p+1}\sin\frac{2cb_u\pi}{n}$	$-2\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}$
98	8	puisqu'ici	jusqu'ici
98	dernière	$\sum_{y=0}^{x=n}$	$\sum_{x=0}^{x=n}$
99	dernière	;	.
109	1	congruenc	congruence
122	11	$\frac{nN_1-n+1}{a}$;	$\frac{nN_1-n+1}{a}$;
125	4, 5 et 7	$\sum_{y=0}^{y=n}$	$\sum_{y=1}^{y=n}$
126	6 en rem.	équation	équation
128	8 en rem.	principe	principe de

PAGES.	LIGNES.	FAUTES.	CORRECTIONS.
141	14 en rem.	équations	équation
141	7 en rem.	an	au
149	3 en rem.	équatiou	équation
154	10	$+\left(d+\frac{t}{s}\right)^2$	$+\left(d+\frac{t}{p}\right)^2$
159	4	$-\left(\frac{m}{6p^2}\right)^3$	$-\left(\frac{m}{6q^2}\right)^3$
165	4	à	a
167	2	laquel	lequel
171	2	équations	équation
173	11	répèterons	répéterons
175	3 en rem.	solution	solutions
178	11	bx^{m-1}	bx^{pn-1}
178	13	$Aqy^n \sqrt[n]{1+\frac{s}{A^n q^m y^{mn}}}$, . . .	$Aqy^m \sqrt[n]{1+\frac{s}{A^n q^n y^{mn}}}$,
179	3	$ay^m \sqrt{1+\frac{f(x,y)}{a^n y^{mn}}}$	$ay^m \sqrt[n]{1-\frac{f(x,y)}{a^n y^{mn}}}$
179	3	$ay^m\left(1+\frac{f(x,y)}{na^n y^{mn}}-\text{etc.}\right)$, . .	$ay^m\left(1-\frac{f(x,y)}{na^n y^{mn}}+\text{etc.}\right)$,
179	9	même	même tems
180	2 en rem.	$-(4ay^n+by^{n-1}\ldots+cy+d)$	$-4(ay^n+by^{n-1}\ldots+cy+d)$
181	10 en rem.	régardent	regardent
183	3	équations $\frac{a}{b}$	équation $\frac{a}{c}$
186	11	de signes	des signes
195	4 en rem.	connnes	connues
202	1	*Memoire*	*Mémoire*

